RECORD AND BRIEFS.

Supreme Court, U.S.
FILED
JUN 23 2017
OFFICE OF THE CLERK

17-2

No.

In the Supreme Court of the United States

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

UNITED STATES OF AMERICA, PETITIONER

v.

MICROSOFT CORPORATION

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

JEFFREY B. WALL
Acting Solicitor General
Counsel of Record
KENNETH A. BLANCO
Acting Assistant Attorney General
MICHAEL R. DREEBEN
Deputy Solicitor General
ELAINE J. GOLDENBERG
Assistant to the Solicitor General
ROSS B. GOLDMAN
Attorney
Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

Library of Congress
Law Library

QUESTION PRESENTED

Whether a United States provider of email services must comply with a probable-cause-based warrant issued under 18 U.S.C. 2703 by making disclosure in the United States of electronic communications within that provider's control, even if the provider has decided to store that material abroad.

PARTIES TO THE PROCEEDING

Petitioner is the United States of America, which was appellee in the court of appeals. Respondent is Microsoft Corporation, which was appellant in the court of appeals.

TABLE OF CONTENTS

Page

Opinions below 1
Jurisdiction 2
Statutory provisions involved 2
Statement 2
Reasons for granting the petition 12
A. The panel's decision is wrong 13
B. The panel's decision conflicts with the framework of analysis in this Court's extraterritoriality decisions and with lower-court decisions addressing a subpoena recipient's duties 21
C. The panel's decision gravely threatens public safety and national security 26
Conclusion 33
Appendix A — Court of appeals opinion (July 14, 2016) 1a
Appendix B — Magistrate judge memorandum and order (Apr. 25, 2014) 73a
Appendix C — Excerpt from corrected hearing transcript (July 31, 2014) 99a
Appendix D — District court order (Aug. 12, 2014) 102a
Appendix E — District court order (Sept. 8, 2014) 103a
Appendix F — Court of appeals order denying rehearing en banc (Jan. 24, 2017) 105a
Appendix G — Statutory provisions 155a

TABLE OF AUTHORITIES

Cases:

Braswell v. *United States*, 487 U.S. 99 (1988) 24
Hay Grp., Inc. v. *E.B.S. Acquisition Corp.*, 360 F.3d 404 (3d Cir. 2004) 24
Henson v. *Santander Consumer USA Inc.*, No. 16-349 (June 12, 2017) 21

Cases—Continued: Page

Information Associated with One Yahoo Email Address That Is Stored at Premises Controlled by Yahoo, In re, No. 17-M-1234, 2017 WL 706307 (E.D. Wis. Feb. 21, 2017) 25
Marc Rich & Co. v. *United States*, 707 F.2d 663 (2d Cir.), cert. denied, 463 U.S. 1215 (1983) 6, 23
Morrison v. *National Austl. Bank Ltd.*, 561 U.S. 247 (2010) 13, 14, 16, 21, 22
New Jersey v. *City of New York*, 283 U.S. 473 (1931) 24
RJR Nabisco, Inc. v. *European Cmty.*, 136 S. Ct. 2090 (2016) ..... *passim*
SEC v. *Minas de Artemisa, S. A.*, 150 F.2d 215 (9th Cir. 1945) 24
Sealed Case, In re, 832 F.2d 1268 (D.C. Cir. 1987) 23
Search Warrant No. 16-960-M-01 to Google, In re, No. 16-960-M-01, 2017 WL 471564 (E.D. Pa. Feb. 3, 2017) 25, 27, 30
Société Nationale Industrielle Aérospatiale v. *United States Dist. Court*, 482 U.S. 522 (1987) 24
Soldal v. *Cook Cnty.*, 506 U.S. 56 (1992) 20
Superintendent of Ins. of N.Y. v. *Bankers Life & Cas. Co.*, 404 U.S. 6 (1971) 14, 16
The Search of Content That Is Stored at Premises Controlled by Google, In re, No. 16-mc-80263, 2017 WL 1398279 (N.D. Cal. Apr. 19, 2017) 25, 28
The Search of Info. Associated with [Redacted]@Gmail.com That Is Stored at Premises Controlled by Google, Inc., In re, No. 16-mj-757 (D.D.C. June 2, 2017) 25

Cases—Continued: Page

The Search of Premises Located at [Redacted]@yahoo.com Stored at Premises Owned, Maintained, Controlled, or Operated by Yahoo, Inc., In re, No. 17-mj-1238 (M.D. Fla. Apr. 7, 2017) 25
United States v. *Bank of Nova Scotia*, 740 F.2d 817 (11th Cir. 1984), cert. denied, 469 U.S. 1106 (1985) 23

Constitution, statutes, and regulations:

U.S. Const. Amend. IV 8, 31
Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 ..... 4, 19
§ 201, 100 Stat. 1861 15
Stored Communications Act, Pub. L. No. 99-508, Tit. II, § 201, 100 Stat. 1860 (18 U.S.C. 2701 *et seq.*) ... 4, 12
18 U.S.C. 2701-2712 4
18 U.S.C. 2701 ..... 7, 16, 155a
18 U.S.C. 2701(c)(1) 17, 156a
18 U.S.C. 2702 ..... 7, 156a
18 U.S.C. 2702(a) 16, 156a
18 U.S.C. 2702(b)(2) 16, 157a
18 U.S.C. 2703 ..... *passim*, 160a
18 U.S.C. 2703(a) 4, 160a
18 U.S.C. 2703(a)-(c) 4, 15, 160a
18 U.S.C. 2703(b) 4, 160a
18 U.S.C. 2703(b)(1) 15, 160a
18 U.S.C. 2703(d) 4, 15, 163a
18 U.S.C. 2703(e) 15, 164a
18 U.S.C. 2703(f) 16, 164a
18 U.S.C. 2703(g) 4, 16, 23, 164a
18 U.S.C. 2705 4

Statutes and regulations—Continued: Page

18 U.S.C. 2707 7
18 U.S.C. 2711(4) 14, 166a
Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, Tit. II, § 212, 115 Stat. 284 ..... 14, 15
18 U.S.C. 1962 21
18 U.S.C. 1964 21
Parliament and Council Regulation 2016/679, 2016 O.J. (L 119) (EU):
Art. 46 33
Art. 48 ..... 32, 33
Art. 49 33

Miscellaneous:

Orin Kerr, *The Surprising Implications of the Microsoft/Ireland Warrant Case*, Wash. Post, Nov. 29, 2016, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/29/the-surprising-implications-of-the-microsoftireland-warrant-case/ 27
Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531 (2005) 18
Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearing Before the S. Subcomm. on Crime & Terrorism (May 24, 2017) (available at https://www.judiciary.senate.gov/meetings/law-enforcement-access-to-data-stored-across-borders-facilitating-cooperation-and-protecting-rights):
Statement of Brad Wiegmann, Deputy Assistant Attorney General, DOJ 28, 29, 30

Miscellaneous—Continued: Page

Written Statement of Christopher W. Kelly, Digital Evidence Laboratory Dir., Assistant Attorney General, Office of the Massachusetts Attorney General 29

Written Testimony of Brad Smith, President and Chief Legal Officer, Microsoft Corp. 32

In the Supreme Court of the United States

No.

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

UNITED STATES OF AMERICA, PETITIONER

v.

MICROSOFT CORPORATION

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SECOND CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

The Acting Solicitor General, on behalf of the United States, respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Second Circuit in this case.

OPINIONS BELOW

The opinion of the court of appeals (App., *infra*, 1a-72a) is reported at 829 F.3d 197. The order denying rehearing en banc and the opinions concurring in and dissenting from that denial (App., *infra*, 105a-154a) are reported at 855 F.3d 53. The orders of the district court judge (App., *infra*, 99a-103a) are unreported. The opinion of the magistrate judge (App., *infra*, 73a-98a) is reported at 15 F. Supp. 3d 466.

JURISDICTION

The judgment of the court of appeals was entered on July 14, 2016. A timely petition for rehearing was denied on January 24, 2017 (App., *infra*, 105a-154a). On April 12, 2017, Justice Ginsburg extended the time within which to file a certiorari petition to and including May 24, 2017. On May 15, 2017, Justice Ginsburg further extended the time within which to file a petition to and including June 23, 2017. This Court's jurisdiction is invoked under 28 U.S.C. 1254(1).

STATUTORY PROVISIONS INVOLVED

The relevant statutory provisions are reproduced in the appendix to this petition. App., *infra*, 155a-166a.

STATEMENT

Under long-standing principles, the recipient of a subpoena to produce documents to the government in the United States is required to produce specified materials within its control, even if the recipient chooses to store those materials abroad. Providers of email services have long adhered to the same approach and have produced foreign-stored data when served with probable-cause-based warrants requiring disclosure of emails to the government in the United States under 18 U.S.C. 2703. In this case, the Second Circuit upended that practice by interpreting such a warrant to call for an impermissible extraterritorial application of the statute. That holding is wrong, inconsistent with this Court's framework for analysis of extraterritoriality issues, and highly detrimental to criminal law enforcement. The Second Circuit denied rehearing by a 4-4 vote, with each of the dissenters writing to identify the panel's legal errors and the deleterious conse-

quences of its decision. This Court's review and reversal is warranted.

1. a. Microsoft is a United States corporation, incorporated and headquartered in Washington State, that operates free, web-based email services such as "MSN" and "Hotmail." See App., *infra*, 5a & n.1. The company stores the contents of users' emails—along with various other information associated with users' email accounts, such as IP addresses and lists of contacts—on a network of approximately one million servers. See *id.* at 6a-7a. Those servers are housed in approximately 100 datacenters located in 40 countries. See *id.* at 7a.

When a user signs up for a Microsoft email service, he is asked to identify where he is "from." C.A. App. A36; see App., *infra*, 6a. Microsoft does not verify his location. See App., *infra*, 7a. Rather, Microsoft runs an automatic scan on newly created accounts and then "migrate[s]" the account data to a datacenter near the user's reported location. C.A. App. A36-A37.

One of Microsoft's datacenters is located in Dublin, Ireland. See App., *infra*, 7a. When Microsoft migrates email content and other account information to the Dublin datacenter, the company deletes the content and much of the other information from its domestic servers (while keeping several copies of the content in other places outside the United States for "redundancy"). C.A. App. A37. Only three "data sets" remain in the United States after the deletion: "some non-content email information"; "some information about the user's online address book"; and "some basic account information, including the user's name and country" as reported by the user. App., *infra*, 7a-8a; see C.A. App. A36-A38.

b. In December 2013, the government applied for a warrant requiring Microsoft to disclose email information for a particular user's email account. See App., *infra*, 2a, 8a-10a. The government's application established probable cause to believe that the account was being used to conduct criminal drug activity. See *id.* at 2a.

The legal basis for requiring such disclosure is found in 18 U.S.C. 2703, which is part of Title II of the Electronic Communications Privacy Act of 1986—generally called the Stored Communications Act (SCA). See 18 U.S.C. 2701-2712; see also App., *infra*, 12a. Section 2703 creates authority for the government to require a provider of an electronic communication service or remote computing service to disclose content and non-content information to the government about a wire or electronic communication. One such authority is a "warrant issued using the procedures described in the Federal Rules of Criminal Procedure * * * by a court of competent jurisdiction." 18 U.S.C. 2703(a) (covering content stored by an electronic communication service); see 18 U.S.C. 2703(b) (covering content stored by a remote computing service); see also 18 U.S.C. 2703(g) (presence of an officer is not required for service or execution of a warrant for disclosure under Section 2703).[1]

A federal magistrate judge issued the requested warrant under Section 2703, concluding that the gov-

---

[1] The government can also in certain circumstances "require the disclosure" of "a record or other information pertaining to a subscriber to or customer of such service," as well as certain categories of content information, not only pursuant to a warrant but also by means of a subpoena or court order. 18 U.S.C. 2703(a)-(c); see 18 U.S.C. 2703(d), 2705.

ernment had established probable cause to believe that the specified email account was being used in narcotics trafficking. See App., *infra*, 2a. The warrant covered "information associated with" an MSN.com email account "stored at premises owned, maintained, controlled, or operated by Microsoft Corporation." *Id.* at 9a (citation omitted). The warrant required Microsoft to "disclose * * * to the Government" the contents of emails stored in the account and some additional records "regarding the identification of the account," including the name and IP addresses associated with the account and the user's contact list. Warrant Attach. C.

Microsoft was served with the warrant at its headquarters in Redmond, Washington. See App., *infra*, 2a. In response, Microsoft disclosed the account-identification records, which it stored in the United States. But the company refused to disclose the contents of the emails in the account, which it had "migrat[ed]" to its datacenter in Ireland. *Id.* at 7a, 10a. Although Microsoft had made a business decision to store the emails abroad, it retained the capability of readily accessing and moving the emails to the United States by using a "database management [computer] program," *id.* at 8a, operated by U.S. employees. Nevertheless, Microsoft moved to quash the warrant as to material stored abroad, arguing (*inter alia*) that it would be an impermissible extraterritorial application of the statute to require Microsoft to disclose information stored outside this country. See *id.* at 20a-21a, 73a-74a.

The magistrate judge denied the motion to quash. He explained that, while a Section 2703 warrant is "obtained" like a "conventional warrant" on a showing of probable cause, it operates like a subpoena because "it

is served on the [provider] in possession of the information and does not involve government agents entering the premises of the [provider] to search its servers and seize the e-mail account in question." App., *infra*, 84a. He concluded that Section 2703 does not "alter the basic principle"—which has "long been the law" with respect to subpoenas—that "an entity lawfully obligated to produce information" in its control "must do so regardless of the location of that information." *Id.* at 84a-85a (citing *Marc Rich & Co.* v. *United States*, 707 F.2d 663, 667 (2d Cir.), cert. denied, 463 U.S. 1215 (1983)). He also noted that "the concerns that animate the presumption against extraterritoriality are simply not present here" because Section 2703 does not punish conduct occurring outside the United States, does not require the presence of government personnel or provider employees abroad, and "places obligations only on the service provider to act within the United States." *Id.* at 92a-93a.

On de novo review, the district court affirmed the magistrate judge's ruling. See App., *infra*, 102a. Based on a joint stipulation of the parties designed to ensure appellate jurisdiction, the court held Microsoft in civil contempt for its refusal to comply with the warrant. See *id.* at 103a.

2. a. A panel of the court of appeals reversed the denial of the motion to quash and vacated the civil contempt finding. The panel ruled that enforcing the warrant as to information stored abroad would constitute an impermissible extraterritorial application of Section 2703. See App., *infra*, 1a-48a.

Citing *RJR Nabisco, Inc.* v. *European Community*, 136 S. Ct. 2090 (2016), the panel concluded that Section 2703 does not apply extraterritorially. See App., *infra*,

23a-36a. Accordingly, the panel considered "the 'focus' of the relevant statutory provision," *id.* at 36a, to determine whether "conduct relevant to the statute's focus occurred in the United States," in which case the warrant "involves a permissible domestic application" of the statute "even if other conduct occurred abroad," *RJR Nabisco*, 136 S. Ct. at 2101.

The panel concluded that in this case the conduct relevant to Section 2703's focus occurred outside the United States. In the panel's view, the relevant statutory focus is maintaining the privacy of a user's email communications and "the invasion of the customer's privacy takes place * * * where the customer's protected content" is stored—here, in the Dublin datacenter. App., *infra*, 43a. The panel grounded its identification of a "privacy" focus in Section 2703's "appear[ance] in a statute entitled the Electronic Communications Privacy Act"; Section 2703's reference to the rules for issuance of warrants in the Federal Rules of Criminal Procedure; a reading of Sections 2701, 2702, and 2707 of the SCA, which relate to privacy; and legislative history showing that protection of privacy was a goal of the SCA. *Id.* at 37a-43a. As to the conclusion that invasion of privacy takes place where the data is stored, the panel asserted that a warrant requiring a provider to access a datacenter abroad calls for the provider to "seize[]" the data from that location while "acting as an agent of the government." *Id.* at 43a-44a.

b. Judge Lynch concurred in the judgment, describing "the sole issue" in the case as "whether Microsoft can thwart the government's otherwise justified demand for the emails at issue by the simple expedient of choosing—in its own discretion—to store

them on a server in another country." App., *infra*, 52a. He disagreed with the notion that the Section 2703 warrant in this case involves a "threat to individual privacy," *id.* at 49a, pointing out that a judge found probable cause "consistent with the highest level of protection" under the Fourth Amendment. *Id.* at 50a. He disapproved of an analysis of Section 2703 under which the propriety of a warrant depends on "the business decisions of a private corporation." *Id.* at 53a. And he stated that a Section 2703 warrant "does not operate like a traditional arrest or search warrant" and that deeming such a warrant to invade privacy in the location where "private content is stored" is a "suspect" conclusion. *Id.* at 62a n.6, 65a n.7. He nevertheless concurred in the judgment, despite "considerable" hesitation, on the ground that Congress did not "demonstrate[] a clear intention to reach situations" in which data is stored abroad. *Id.* at 66a-67a; see *id.* at 65a n.7. He made clear, however, that he harbored no "illusion that" the court's holding "should * * * be regarded as a rational policy outcome, let alone celebrated as a milestone in protecting privacy." *Id.* at 72a.

3. The government petitioned for rehearing en banc. By an evenly divided 4-4 vote, with several judges recused and Judge Lynch ineligible to participate because he had recently taken senior status, the court of appeals denied the petition. See App., *infra*, 105a & n.*, 107a n.1. Judge Carney, who authored the panel's decision, concurred in the denial of rehearing. See *id.* at 107a-119a. Judges Cabranes, Raggi, Droney, and Jacobs each dissented from the denial (and joined each other's dissents). See *id.* at 120a-154a.

a. Judge Cabranes explained that the panel's ruling "has indisputably, and severely, restricted an essential investigative tool used thousands of times a year in important criminal investigations around the country," while failing to "serve any serious, legitimate, or substantial privacy interest." App., *infra*, 125a (citation, brackets, and internal quotation marks omitted). He concluded that this case "presents multiple questions of exceptional importance to public safety and national security," *id.* at 124a, and that the panel's decision should be "rectified as soon as possible by a higher judicial authority" or by Congress, *id.* at 137a; see *id.* at 137a n.37 (noting that the possibility of congressional action is "entirely speculative").

Judge Cabranes detailed a number of "far reaching" harmful effects of the panel's decision. App., *infra*, 125a. First, he stated, that decision "has substantially burdened the government's legitimate law enforcement efforts" by preventing enforcement of a warrant requiring a service provider to "turn over emails stored in servers located outside the United States," even if the government is certain that the emails contain evidence of a "terrorist plot" or other serious criminal wrongdoing. *Id.* at 125a-126a (citation omitted). Second, he observed, the decision has "created a roadmap for the facilitation of criminal activity," since it allows even an "unsophisticated" criminal in the United States to shield emails from the government's view by falsely reporting a foreign residence when signing up for Microsoft email service. *Id.* at 125a-127a. Third, he explained, the decision has "impeded programs to protect the national security of the United States and its allies" by leading "major service providers to reduce significantly their cooperation with

law enforcement" so as to "radically undermine the effectiveness of an SCA warrant." *Id.* at 125a, 127a-128a; see *id.* at 127a-129a (explaining that some providers break information up across different locations, move it frequently, or cannot determine where particular data is stored).

Judge Cabranes also stated that "[t]he baleful consequences of the panel's decision" are based on a "flawed reading" of the statute. App., *infra*, 129a, 135a n.35; see *id.* at 131a n.22. Even assuming that the relevant statutory focus is "user privacy," he reasoned, "a plain reading of the statute makes clear that the conduct relevant to" that focus "is a provider's *disclosure* or *non-disclosure* of emails to third parties, not a provider's *access* to a customer's data." *Id.* at 132a. Judge Cabranes pointed out that the SCA recognizes a provider's right to access a user's communications, that such access does not invade a user's privacy unless the provider divulges the communications to someone else, and that Microsoft has lawful possession of the relevant emails and the ability to access those emails at its U.S. headquarters. See *id.* at 129a n.19, 135a-136a; see also *id.* at 124a-125a; 130a n.19 (explaining that "a disclosure warrant is * * * akin to a subpoena," albeit "with the important added protection of a probable cause showing to a neutral magistrate"). Because disclosure of the emails to the government would take place in the United States, Judge Cabranes concluded, enforcement of the warrant in this case is a domestic application of Section 2703. See *id.* at 136a; see also *id.* at 132a.

b. Judge Raggi also emphasized the exceptional importance of this case and the "immediate and serious adverse consequences" of the panel's ruling. App.,

infra, 139a. "On the panel's reasoning," she explained, if the government had been able to show in early September 2001 probable cause to believe that the 9/11 perpetrators "were communicating electronically about an imminent, devastating attack on the United States, and that Microsoft possessed those emails," a federal court would not have been able to issue a Section 2703 warrant if Microsoft had stored the emails outside the United States, "even though [Microsoft's] employees would not have had to leave their desks in Redmond, Washington, to retrieve them." *Id.* at 138a n.1.

On the merits, Judge Raggi agreed with Judge Cabranes that the panel's extraterritoriality analysis is erroneous, even assuming that Section 2703's focus is "privacy," because privacy is not invaded by "Microsoft's access of its own files in Dublin" but only by "disclosure of subscriber communications in the United States." App., *infra*, 146a-147a; see *id.* at 145a. She explained that a Section 2703 warrant "is executed with respect to * * * the person ordered to divulge materials in his possession," not with respect to a place, and thus operates domestically when such a person is "within United States territory and subject to the court's jurisdiction." *Id.* at 141a; see *id.* at 143a.

c. Judges Droney and Jacobs echoed the analysis in the other dissents. Judge Droney stressed that an extraterritoriality analysis must take place "provision by provision"; that "the activity that is the focus of the disclosure aspects of the SCA would necessarily occur in the United States where Microsoft is headquartered * * * , not in the foreign country where it has chosen to store the electronic communications of its customers" based on "its own business considerations"; and

that the warrant requirement protects privacy while allowing "important criminal investigations" to proceed. App., *infra*, 150a-152a. Judge Jacobs explained that "[t]he warrant in this case can reach what it seeks because the warrant was served on Microsoft, and Microsoft has access to the information sought" and "need only touch some keys in Redmond, Washington." *Id.* at 121a.

REASONS FOR GRANTING THE PETITION

The Second Circuit has seriously misinterpreted the Stored Communications Act (SCA). In the panel's view, the government cannot require a U.S. service provider to disclose to the government, in the United States, emails and related information that the provider, for its own business reasons, has stored abroad. The panel reached that unprecedented holding by reasoning that such a disclosure would be an extraterritorial application of the Act—even though the warrant requires disclosure in the United States of information that the provider can access domestically with the click of a computer mouse. The panel's decision is incorrect: the SCA's requirement that a provider disclose information to the government in the United States is a domestic, not an extraterritorial, application. The panel's contrary conclusion conflicts with this Court's framework for resolving extraterritoriality questions and with the unanimous holdings of courts that a domestic recipient of a subpoena is required to produce specified materials within the recipient's control, even if the recipient stores the materials abroad.

As the dissenters from denial of en banc review explained, the decision is causing immediate, grave, and ongoing harm to public safety, national security, and the enforcement of our laws. Under this opinion, hun-

dreds if not thousands of investigations of crimes—ranging from terrorism, to child pornography, to fraud—are being or will be hampered by the government's inability to obtain electronic evidence. And the opinion cannot be defended as a protection of privacy. The government established probable cause to believe that the communications would provide evidence of a crime, thus meeting constitutional standards for a warrant. The decision protects only criminals whose communications are placed out of reach of law enforcement officials because of the business decisions of private providers. Nothing in the language or structure of the SCA, or in this Court's precedents, justifies that anomalous consequence. This Court should grant certiorari and reverse the decision below.

A. The Panel's Decision Is Wrong

1. "Absent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application." *RJR Nabisco, Inc.* v. *European Cmty.*, 136 S. Ct. 2090, 2100 (2016) (citing *Morrison* v. *National Austl. Bank Ltd.*, 561 U.S. 247, 255 (2010)). But the existence of foreign conduct in a statute's application does not mean that the law in question is being applied extraterritorially. See *id.* at 2101. Other conduct may make the application domestic.

To determine whether a case involves a "permissible domestic application" of a statutory provision, a court must "look[] to the * * * 'focus'" of the provision at issue. *RJR Nabisco*, 136 S. Ct. at 2101. "If the conduct relevant to the statute's focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad; but if the conduct relevant to the focus occurred in a foreign country, then the case involves an

* * * extraterritorial application regardless of any other conduct that occurred in U.S. territory." *Ibid.*

A court ascertains the focus of a particular statutory provision by identifying the acts that the provision "seeks to 'regulate'" and the parties or interests that it "seeks to 'protec[t].'" *Morrison*, 561 U.S. at 267 (quoting *Superintendent of Ins. of N.Y.* v. *Bankers Life & Cas. Co.*, 404 U.S. 6, 10, 12 (1971)); see *RJR Nabisco*, 136 S. Ct. at 2100-2101. Because different provisions in the same enactment may have different focuses, see, *e.g.*, *RJR Nabisco*, 136 S. Ct. at 2108, 2110-2111, the analysis must proceed on a provision-by-provision basis.

2. Applying that analysis to Section 2703 leads "inexorably" to the conclusion that the provision is applied domestically when a court issues a warrant to a provider in the United States requiring disclosure in this country of material over which the provider has control, regardless of whether the provider stores that material abroad. App., *infra*, 133a (Cabranes, J., dissenting).[2]

a. i. Contrary to the panel's conclusion, Section 2703 focuses on a provider's *disclosure* of electronic communications to the government in the United States. See 18 U.S.C. 2703, 2711(4); see also, *e.g.*, App., *infra*, 145a (Raggi, J., dissenting); *id.* at 60a-62a (Lynch, J., concurring in the judgment). And that required disclosure is a domestic act.

Section 2703's regulatory regime centers on procedures and standards for requiring disclosure of information to the government. See Pub. L. No. 107-56, Tit. II, § 212, 115 Stat. 284-285 (2001) (Section 2703 is

---

[2] References to "dissenting" opinions in this brief are to the dissents from the denial of rehearing en banc.

captioned "Required disclosure of customer communications or records").[3] Section 2703 defines when the government can require disclosure of the content of electronic communications, or other records relating to such communications, pursuant to a warrant. Under Section 2703, "[a] governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication" pursuant to a warrant; "[a] governmental entity may require a provider of remote computing service to disclose the contents" of certain communications if the entity "obtains a warrant"; and "[a] governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber" by obtaining a warrant, in which case the "provider * * * shall disclose" the information. 18 U.S.C. 2703(a)-(c).

Section 2703 also contains other procedures regulating disclosure, underscoring the provision's disclosure-oriented focus. Under certain circumstances, Section 2703 requires the provider to "disclose" information under process other than a warrant. 18 U.S.C. 2703(b)(1) and (d); see 18 U.S.C. 2703(a)-(c). It protects providers from suit for "providing information" under a disclosure order. 18 U.S.C. 2703(e). It mandates that providers preserve electronic communications and records at the government's request, so that the material is available for later disclosure to the gov-

---

[3] Before Congress amended Section 2703 in 2001 (in a part of the enactment called "emergency disclosure of electronic communications to protect life and limb," § 212, 115 Stat. 284), that provision was captioned "Requirements for governmental access." Pub. L. No. 99-508, § 201, 100 Stat. 1861.

ernment. See 18 U.S.C. 2703(f). And it states that the presence of an officer is not required for service or execution of a warrant "requiring disclosure." 18 U.S.C. 2703(g).

By repeatedly emphasizing the requirement of disclosure, the text of Section 2703 makes clear that the provision "seeks to 'regulate'" disclosure to the government and "to 'protec[t]'" the government's ability to obtain such disclosure. *Morrison*, 561 U.S. at 267 (quoting *Superintendent of Ins. of N.Y.*, 404 U.S. at 10, 12). In this way, Section 2703 differs from provisions of the SCA directed at preventing access to information. For instance, Section 2701 punishes unlawful access to electronic communications or facilities, see 18 U.S.C. 2701, and Section 2702(a) bars a provider from "knowingly divulg[ing]" the contents of an electronic communication, 18 U.S.C. 2702(a); see 18 U.S.C. 2702(b)(2) (exception for disclosures authorized in Section 2703). Section 2703, in contrast, focuses on situations in which governmental interests in obtaining the information overcome users' privacy interests—including when the information is needed for a criminal investigation and the government has met the applicable standards for disclosure.

Because the "conduct relevant to [the SCA's] focus" occurs in this country, the existence of "other conduct" that "occur[s] abroad" does not alter the conclusion that the case "involves a permissible domestic application" of the provision in question. *RJR Nabisco*, 136 S. Ct. at 2101. Here, issuance and enforcement of a warrant requiring a provider in the United States to disclose information to the government in the United States involves domestic conduct within the focus of Section 2703. It thus constitutes a domestic applica-

tion of that provision. See Warrant 1; App., *infra*, 146a-147a (Raggi, J., dissenting).

ii. Even assuming that the panel's decision correctly identified "privacy" as the focus of Section 2703, the conduct relevant to any privacy focus takes place in the United States, where disclosure to the government occurs. Accordingly, treating privacy as a focus of Section 2703 would result in the same conclusion: compliance with an SCA warrant requiring disclosure of information in the United States is a domestic, not an extraterritorial, act.

The SCA "protects user privacy by prohibiting unlawful access of customer communications * * * and by regulating a provider's *disclosure* of customer communications to third parties." App., *infra*, 135a (Cabranes, J., dissenting). A provider's internal access to electronic communications to comply with the SCA does not implicate a user's privacy. A provider already has a right to possess a user's communications and does not need any additional legal authorization to shift stored communications from one country to another. See, *e.g.*, 18 U.S.C. 2701(c)(1) (exempting providers from rules against unlawful access to stored communications). And a user's privacy is not invaded when a provider does so.

In this case, for instance, Microsoft was not restricted from migrating the account from the United States to Ireland, and Microsoft was not restricted from bringing it back. Microsoft "already had possession of, and lawful *access* to, the targeted emails from its office in Redmond, Washington," and no warrant was required for Microsoft to "move the emails from Ireland to the United States." App., *infra*, 136a (Cabranes, J., dissenting). The user of Microsoft's

service has no recourse, or even entitlement to notice, if the provider decides for its own private business reasons to transfer the user's stored communications into or out of the United States. See *id.* at 144a-145a, 147a (Raggi, J., dissenting) (Microsoft "did not need the approval of Irish authorities or even of its subscriber to take such action").

Under those circumstances, a user has no protected privacy interest in whether a provider keeps the records of his electronic communications in the United States or abroad, or in whether the provider moves the information from one location to another. When a Section 2703 warrant issues, any statutory concern with a user's privacy arises only when the provider discloses the information covered by the warrant to the government so that the government can search it, a step that would generally be "unlawful under the SCA absent a warrant." App., *infra*, 136a (Cabranes, J., dissenting); see *id.* at 146a (Raggi, J., dissenting); see also, *e.g.*, Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 551 (2005). The provider's antecedent conduct of gathering responsive material is not the relevant statutory event. Disclosure to the government is the conduct relevant to a privacy focus—and that disclosure happens domestically, not in a foreign location where the provider has decided to store the communications. See App., *infra*, 146a-147a (Raggi, J., dissenting).

iii. More broadly, in this case the government has invoked Section 2703 to regulate the conduct of a U.S. company that is doing business in the United States and that is subject to process in the United States. Having taken full advantage of the protections of U.S. law, Microsoft should not be permitted to evade the

requirements of Section 2703 in the United States simply by the expedient of shifting data to storage devices that it locates abroad. See App., *infra*, 152a (Droney, J., dissenting) (stating that "it is the location of the provider of the electronic communication service that is relevant to determining whether the SCA is being applied extraterritorially"). To allow that result permits a private provider in the United States to thwart Section 2703's critical role in assisting law enforcement to combat domestic terrorism and crime.

b. In reaching a contrary result, the panel provided no sound justification. See App., *infra*, 135a n.35 (Cabranes, J., dissenting) (stating that the panel majority and the en banc concurrence "fail to explain" key points).

First, the panel's decision located little support in Section 2703 for identifying its focus as privacy. The decision instead relies heavily on the name of the statute in which the SCA appears (the Electronic Communications Privacy Act), on legislative history showing that Congress was generally concerned about privacy, and on the existence of SCA provisions other than Section 2703 that aim at protecting privacy. See App., *infra*, 37a-43a. That analysis fails. Congress's background concern with privacy, and its enactment of other provisions addressed to that concern, does not mean that Section 2703 itself focuses on privacy—rather than on (as the text of Section 2703 indicates) situations justifying disclosure and the procedures for requiring it.

Second, the panel was wrong in asserting that a provider's decision to access data stored in its foreign data centers represents the conduct relevant to a privacy focus. The panel's entire discussion of the point

consists of the statement that "it is our view that the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed—here, where it is seized by Microsoft, acting as an agent of the government." App., *infra*, 43a-44a. But the panel cited nothing in the SCA to justify its assertion that an intra-company transfer of a customer's data invades the customer's privacy. A provider does not act as a government agent, or "seize" records, by accessing and transferring material of which it is already in possession and which it is free to move among storage locations at any time. See *id.* at 144a-145a, 147a (Raggi, J., dissenting); *id.* at 134a n.30 (Cabranes, J., dissenting); see also, *e.g.*, *Soldal* v. *Cook Cnty.*, 506 U.S. 56, 63 (1992) ("A 'seizure' of property occurs where there is some meaningful interference with an individual's possessory interests in that property.") (citation omitted). Microsoft's transfer of information across a fiber-optic cable from one data center to another does not have any impact at all on a user's privacy, let alone compromise his privacy vis-à-vis a third party like the government.

Third, the panel appeared to be influenced by the fact that, when Congress passed the SCA, it did not specifically anticipate that user data might be stored overseas and thus that a provider might have to retrieve information across international boundaries to comply with a Section 2703 warrant. See App., *infra*, 4a-5a; see also *id.* at 108a (Carney, J., concurring in the denial of rehearing en banc) (arguing that "the SCA has been left behind by technology"). But the task of the courts is "to apply faithfully the law Congress has written," regardless of whether the legislature failed to consider a factual circumstance that did

not exist at the time of the law's enactment. *Henson* v. *Santander Consumer USA Inc.*, No. 16-349 (June 12, 2017), slip op. 9; see *Morrison*, 561 U.S. at 261 (stating that courts should avoid "judicial-speculation-made-law—divining what Congress would have wanted if it had thought of the situation before the court"). Mapped onto the warrant in this case, the SCA involves domestic conduct, and its terms remain domestically enforceable notwithstanding changes in the business model of providers.

B. The Panel's Decision Conflicts With The Framework Of Analysis In This Court's Extraterritoriality Decisions And With Lower-Court Decisions Addressing A Subpoena Recipient's Duties

1. The panel's decision is inconsistent with this Court's guidance on how to assess whether a statutory provision is being applied extraterritorially. As explained above, the decision's analysis of the focus of Section 2703 sidesteps the text of that provision and emphasizes general features of the statute of which Section 2703 is a part. See App., *infra*, 37a-43a. But this Court has required a more discriminating analysis—one that assesses the "focus" of the particular statutory provision at issue, rather than the overall focus of the larger statutory scheme that includes that provision.

The Court applied such a provision-specific analysis in *RJR Nabisco*. That decision considered the extraterritoriality of 18 U.S.C. 1962, a provision proscribing certain racketeering conduct, and 18 U.S.C. 1964, a provision stating that "[a]ny person injured in his business or property" by reason of a RICO violation may bring suit. 136 S. Ct. at 2099-2100. The Court ruled that Section 1964 does not apply extraterritorial-

ly and that it "requires a civil RICO plaintiff to allege and prove a domestic injury to business or property," *id.* at 2111—*i.e.*, that such injury is a focus of that provision. The Court emphasized that extraterritoriality analysis "must be applied separately" to other RICO provisions, *id.* at 2108, and did not suggest that those provisions—which do not mention injury to business or property—might have the same focus simply because they are found in the same statute. Cf. *Morrison*, 561 U.S. at 263-265 (ruling that Section 10(b) of the Securities Exchange Act of 1934 does not apply extraterritorially but that Section 30(a) does).

The panel in this case did not properly conduct a provision-by-provision analysis. See, *e.g.*, App., *infra*, 151a (Droney, J., dissenting). And its departure from this Court's framework directly led to its erroneous conclusion. As discussed, the fact that Congress intended the SCA to protect privacy, and included some provisions in sections of the SCA to carry out that purpose, says nothing about the particular focus of Section 2703, which authorizes the government to require providers to disclose certain information. See 18 U.S.C. 2703. The panel's failure to carry out the analysis at the correct level of specificity cannot be reconciled with this Court's decisions.

2. The panel's decision is also inconsistent with settled law on the operation of subpoenas. As the dissenters from denial of en banc rehearing explained, Congress used the term "warrant" in Section 2703 to cover situations in which the government must demonstrate to a neutral judicial officer that it has facts showing the existence of probable cause—a privacy protection of the highest order. But with respect to the disclosure that Section 2703 requires of providers,

a Section 2703 warrant "functions as a subpoena." App., *infra*, 120a (Jacobs, J., dissenting); see *id.* at 130a n.19 (Cabranes, J., dissenting) (a "disclosure warrant is more akin to a subpoena"); *id.* at 58a (Lynch, J., concurring in the judgment) (Section 2703 warrant is not a "traditional search warrant"). Such a warrant does not "authorize federal agents to *search* any premises or to *seize* any person or materials," *id.* at 141a (Raggi, J., dissenting); see 18 U.S.C. 2703(g); it requires nothing more than disclosure of material that a provider in the United States can access and over which it has control, so that the government can review that material once it is in the government's hands.

As numerous courts of appeals have held, a subpoena requiring a person in the United States to produce materials is enforceable regardless of whether the person must retrieve those materials from outside the country. That is because a subpoena "is executed with respect to a person" rather than a place, and therefore operates domestically so long as that person is "within United States territory and subject to the court's jurisdiction." App., *infra*, 141a (Raggi, J., dissenting) (emphasis omitted) (citing *Marc Rich & Co.* v. *United States*, 707 F.2d 663, 668-670 (2d Cir.), cert. denied, 463 U.S. 1215 (1983)); see, *e.g.*, *United States* v. *Bank of Nova Scotia*, 740 F.2d 817, 820-821, 826-829 (11th Cir. 1984) (affirming order enforcing grand jury subpoena requiring disclosure of records located in the Bahamas against a foreign bank subject to the jurisdiction of the district court), cert. denied, 469 U.S. 1106 (1985); *In re Sealed Case*, 832 F.2d 1268, 1270, 1283-1284 (D.C. Cir. 1987) (stating that a subpoena for documents in Switzerland is enforceable if the district

court has personal jurisdiction over the companies whose records are sought), abrogated on other grounds by *Braswell* v. *United States*, 487 U.S. 99 (1988); *SEC* v. *Minas de Artemisa, S. A.*, 150 F.2d 215, 216-218 (9th Cir. 1945) ("The obligation to respond applies even though the person served [with a subpoena] may find it necessary to go to some other place within or without the United States in order to obtain the documents required to be produced."); see also *Hay Grp., Inc.* v. *E.B.S. Acquisition Corp.*, 360 F.3d 404, 412 (3d Cir. 2004) (Alito, J.) (explaining that subpoenaed documents are produced "not [in] the district in which the documents are housed but [in] the district in which the subpoenaed party is required to turn them over").[4]

A Section 2703 warrant likewise governs disclosure by a person rather than access to a place. See App., *infra*, 141a (Raggi, J., dissenting). The panel struggled to reconcile its decision with the decisions of its sister circuits on the enforceability of subpoenas calling for production of material stored abroad, focusing on the private nature of the user's materials sought by the warrant. *Id.* at 30a-36a. But that distinction has nothing to do with the relevant issue: the obligation of

---

[4] Cf. *Société Nationale Industrielle Aérospatiale* v. *United States Dist. Court*, 482 U.S. 522, 538-540, 542-546 (1987) (explaining that a federal court has power to order a foreign party over which it has jurisdiction "to produce evidence physically located within" another nation); *New Jersey* v. *City of New York*, 283 U.S. 473, 482 (1931) (stating that a U.S. court may enter an injunction when "the defendant is before the Court and the property of plaintiff and its citizens that is alleged to have been injured * * * is within the Court's territorial jurisdiction," regardless of whether the "acts creating the nuisance" took place outside the United States).

the recipient to produce data under its control, even if data is stored abroad. See *id.* at 61a n.5 (Lynch, J., concurring in the judgment).

The unsoundness of the panel's analysis is underscored by its rejection, outside the Second Circuit, by all of the magistrate judges to have considered it. Those decisions articulate the principle that "the court may lawfully order" a provider subject to its jurisdiction to "disclose * * * that which it can access and deliver within the United States." *In re Information Associated with One Yahoo Email Address That Is Stored at Premises Controlled by Yahoo*, No. 17-M-1234, 2017 WL 706307, at *7 (E.D. Wis. Feb. 21, 2017).[5] This Court's review is necessary to reaffirm that a person subject to the jurisdiction of a U.S. court cannot strip the court of its authority to require disclosure of materials under that person's control merely by storing them outside the United States.

---

[5] See, *e.g.*, *In re the Search of Content That Is Stored at Premises Controlled by Google*, No. 16-mc-80263, 2017 WL 1398279, at *1, *3-*4 (N.D. Cal. Apr. 19, 2017); *In re the Search of Premises Located at [Redacted]@yahoo.com*, No. 17-mj-1238 (M.D. Fla. Apr. 7, 2017), slip op. 3 (stating that "a warrant issued pursuant to the Act function[s] more like a subpoena in that it requires the provider to disclose information under its control"); see also *In re the Search of Info. Associated with [Redacted]@Gmail.com That Is Stored at Premises Controlled by Google, Inc.*, No. 16-mj-757 (D.D.C. June 2, 2017), slip op. 2, 11, 18, 20 ("[e]very court outside the Second Circuit that has considered the issue has rejected the holding of *Microsoft*"); *In re Search Warrant No. 16-960-M-01 to Google*, No. 16-960-M-01, 2017 WL 471564, at *3, *5 (E.D. Pa. Feb. 3, 2017). Objections to the magistrate judges' decisions are pending.

C. The Panel's Decision Gravely Threatens Public Safety And National Security

1. The panel's decision "has put the safety and security of Americans at risk" by impeding the government's ability to ward off terrorism and similar national-security threats and to investigate and prosecute crimes. App., *infra*, 125a n.6 (Cabranes, J., dissenting). The case therefore raises a question "of exceptional importance to public safety and national security" that warrants this Court's review. *Id.* at 124a; see *id.* at 136a-137a (calling for "a higher judicial authority" to "rectif[y]" the untenable situation created by the panel's decision); *id.* at 139a (Raggi, J., dissenting).

The panel's decision places foreign-stored electronic communications entirely beyond the reach of a Section 2703 warrant despite a neutral judicial officer's determination that probable cause exists to believe that they are evidence of a crime—regardless of the crime's seriousness. As the en banc dissenters explained, barring use of that "essential investigative tool" hampers the government's ability to investigate terrorism and to prevent future attacks. App., *infra*, 125a (Cabranes, J., dissenting) (citation omitted); see *ibid.* (government uses Section 2703 warrants "thousands of times a year") (citation omitted); *id.* at 138a n.1 (Raggi, J., dissenting). It also prevents the government from effectively investigating crimes like child pornography, sex trafficking, drug trafficking, racketeering, and fraud.

The harm caused by the panel's decision is not theoretical, nor is it limited to the Second Circuit or Microsoft. "[T]he major domestic Internet providers aren't treating the Second Circuit's decision as just a decision from one circuit. They have all decided to

treat the * * * decision as the law in effect everywhere." Orin Kerr, *The Surprising Implications of the Microsoft/Ireland Warrant Case*, Wash. Post, Nov. 29, 2016; see App., *infra*, 127a (Cabranes, J., dissenting) ("major service providers" now giving "significantly" reduced cooperation to law enforcement). Thus, although Google previously "routinely complied with federal courts' search warrants [that] commanded the production of user data stored on Google servers located outside the United States," that company now argues that "a warrant issued under the SCA lawfully reaches only data stored within the United States." *In re Search Warrant No. 16-960-M-01 to Google*, No. 16-960-M-01, 2017 WL 471564, at *3-*4 (E.D. Pa. Feb. 3, 2017); see App., *infra*, 127a-128a (Cabranes, J., dissenting). And Yahoo! "has advised law enforcement that it will not even preserve data located outside the United States in response to a [S]ection 2703 request." App., *infra*, 128a-129a (Cabranes, J., dissenting) (citation and internal quotation marks omitted).

The harmful effects of the panel's decision also extend beyond investigations involving the email of foreign nationals. The decision blocks government access to foreign-stored emails even when the user is a U.S. citizen living in the United States who carries out crimes in this country against victims in this country (and the provider is a U.S. business that can access the emails from its U.S. offices at the click of a mouse). As to Microsoft email services, the decision provides a roadmap for terrorists and criminals in the United States to insulate electronic communications from U.S. investigators—they need do nothing more than falsely state a location outside the United States when signing up for an account. See App., *infra*, 125a-127a

(Cabranes, J., dissenting). Other providers, such as Google, store the email content of users in the United States all over the world, moving the location of the data frequently and breaking emails into "shards" so that different portions of a single email may be stored in multiple countries. See *id.* at 127a-128a; see also, *e.g.*, *In re the Search of Content That Is Stored at Premises Controlled by Google*, No. 16-mc-80263, 2017 WL 1398279, at *1-*2 (N.D. Cal. Apr. 19, 2017). Indeed, any provider could, at any time, decide to store all of its data outside the United States as a means of currying favor with its subscribers. Assuming that providers will not take such a step "entrust[s] our national security to the good faith" of those businesses. App., *infra*, 126a n.6 (Cabranes, J., dissenting).

The Second Circuit's decision is therefore "far reaching." App., *infra*, 125a (Cabranes, J., dissenting). The government "is aware of dozens of investigations, across the country, in every judicial circuit," that have been "frustrated" by the panel's decision. *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearing Before the S. Subcomm. on Crime & Terrorism* (May 24, 2017) (*Hearing*) (available at https://www.judiciary.senate.gov/meetings/law-enforcement-access-to-data-stored-across-borders-facilitating-cooperation-and-protecting-rights), Statement of Brad Wiegmann, Deputy Assistant Att'y Gen., DOJ, at 5 (Wiegmann Statement); see *id.* at 3-4. Those investigations include multiple child-exploitation cases in which images attached to emails or otherwise stored by a provider are needed to identify and locate child victims; a drug-trafficking investigation in which email content is needed to identify suppliers and customers;

a tax-fraud investigation in which email content is needed to identify co-conspirators and provide additional evidence of criminal activity; a child-pornography investigation in which email content is needed to help locate a defendant who absconded before trial and remains a fugitive; and a sex-trafficking investigation in which the government was unable to obtain the content of stored photos and videos. See *id.* at 5-6. In many of those cases, "the victim, the offender, and the account holder are all within the United States." *Id.* at 6 (emphasis omitted); see *Hearing*, Written Statement of Christopher W. Kelly, Digital Evidence Lab. Dir., Assistant Att'y Gen., Office of the Mass. Att'y Gen., at 3-4.

2. No sound justification exists for the "baleful consequences," App., *infra*, 129a (Cabranes, J., dissenting), inflicted by the panel's decision.

a. Microsoft has argued that the government need not resort to Section 2703 to obtain electronic communications as part of a criminal investigation. But the government often does not have an effective alternative to requiring disclosure of email that is stored abroad under the SCA.

As to fewer than half of the world's nations, the government has mutual legal assistance treaties (MLATs) that permit U.S. investigators to request that foreign counterparts gather evidence under their own legal procedures. See Wiegmann Statement at 6. But to the extent that an MLAT is applicable in a particular case, the process can be slow and uncertain, often taking many months or even years to generate any result. See, *e.g.*, App., *infra*, 90a-92a; *id.* at 114a n.8 (Carney, J., concurring in denial of rehearing en banc). With respect to certain providers, such as Google, the

MLAT process is entirely futile, because the provider constantly moves data around the world, the location of the data at any given moment in time is difficult or impossible to ascertain, and only the provider's U.S. employees are able to access the information. See, *e.g.*, *In re Search Warrant No. 16-960-M-01 to Google*, 2017 WL 471564, at *14 ("it would be impossible for the Government to obtain the sought-after user data" stored by Google "through existing MLAT channels"); App., *infra*, 127a-128a (Cabranes, J., dissenting); Wiegmann Statement at 6.[6] Thus, under the Second Circuit's decision, data that Google stores abroad is effectively beyond the reach not only of the MLAT process but also of both U.S. and foreign law.

The government has endorsed the development of new legislation that would, among other things, address warrants for electronic communications, and Congress has held hearings on the matter. See, *e.g.*, Wiegmann Statement at 8, 10, 14. But the possibility of future legislation does not reduce the need for this Court's review. Whether (and, if so, when) Congress will enact legislation that addresses the problem presented in this case is highly uncertain. Meanwhile, the government and the public are suffering serious, immediate harms, as the Second Circuit's decision stymies or impedes critical investigations. When a court of appeals decision "has unnecessarily created serious, on-going problems for those charged with enforcing

---

[6] Under the panel's decision, a provider intent on marketing its "privacy" protections to consumers could choose to store information—perhaps based on a user's unverified report of his location—in one of the "many countries," App., *infra*, 127a n.11 (Cabranes, J., dissenting), with which the United States has no MLAT.

the law and ensuring our national security, and where a legislative remedy is entirely speculative," proper interpretation of the "extant statute" remains necessary. App., *infra*, 137a n.37 (Cabranes, J., dissenting); see, *e.g.*, *id.* at 123a (Jacobs, J., dissenting).

b. Microsoft has also argued that the panel's decision protects user privacy. But as the en banc dissenters (and Judge Lynch, concurring in the judgment) explained, "the panel majority's decision does not serve any serious, legitimate, or substantial privacy interest." App., *infra*, 125a (Cabranes, J., dissenting); see *id.* at 72a (Lynch, J., concurring in the judgment) (stating that the panel's result should not be "celebrated as a milestone in protecting privacy" or even "regarded as a rational policy outcome").

That is so for two basic reasons. First, under Section 2703, a user's privacy is fully protected by the government's obligation to obtain a warrant, which can issue only after a neutral judicial officer makes an appropriate finding of probable cause and the warrant specifies with particularity the information to be disclosed. That is equivalent to the "highest level of protection" under the Fourth Amendment. App., *infra*, 50a (Lynch, J., concurring in the judgment). Indeed, "if the government had made an equivalent showing that evidence of a crime could be found in a citizen's home, that showing would permit a judge to authorize law enforcement agents to forcibly enter that home and search every area." *Id.* at 51a.

Second, the panel's decision protects information from the government's view only insofar as private corporations choose to confer that protection. The providers themselves control the location where electronic communications are stored. Thus, had Mi-

crosoft deemed it advantageous to its bottom line to store the content in this case in the United States, then the company would have been obligated without any question to disclose that information pursuant to the Section 2703 warrant. Protection for users that turns on "the business decisions of a private corporation" and may be withdrawn at a provider's whim is little protection at all—and Congress could not have intended such an irrational result in enacting Section 2703. App., *infra*, 53a (Lynch, J., concurring in the judgment).

c. Finally, Microsoft has argued that undoing the panel's decision would harm its business interests and its industry. Those arguments ring hollow. Economic concerns cannot override the text of the statute or the interests in public safety and national security that are at stake in this case—particularly when the claimed economic benefit is derived directly from a provider's ability to market itself as capable of shielding subscribers' activity, including their criminal activity, from discovery by the authorities. In any event, the government seeks only to reinstate the long-standing status quo that existed before the panel issued its decision. In that period, providers readily complied with Section 2703 warrants, regardless of the location in which the requested information was stored, see, *e.g.*, p. 27, *supra*, while their businesses prospered.[7] This

---

[7] Citing Article 48 of the European Union's General Data Protection Regulation (GDPR), which goes into effect in May 2018, Microsoft has suggested that changes in foreign law have significantly altered the risks faced by providers. See *Hearing*, Written Testimony of Brad Smith, President and Chief Legal Officer, Microsoft Corp., at 6; Parliament and Council Regulation 2016/679, 2016 O.J. (L 119) (EU). That is not so. Article 48 does not fore-

Court should grant review to restore the government's ability to require providers to disclose electronic communications—which are, in this day and age, often the only or the most critical evidence of terrorism and crime—pursuant to a Section 2703 warrant.

CONCLUSION

The petition for a writ of certiorari should be granted.

Respectfully submitted.

JEFFREY B. WALL
Acting Solicitor General
KENNETH A. BLANCO
Acting Assistant Attorney General
MICHAEL R. DREEBEN
Deputy Solicitor General
ELAINE J. GOLDENBERG
Assistant to the Solicitor General
ROSS B. GOLDMAN
Attorney

JUNE 2017

---

close disclosure of foreign-stored information by a provider served with a Section 2703 warrant in U.S. territory. Among other things, that Article is "without prejudice" to transfer of data for important public interest purposes, for establishing legal claims, and for "compelling legitimate interests." GDPR Art. 49; see GDPR Arts. 46, 48.

APPENDIX A

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

Docket No. 14-2985
Aug. Term, 2015

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

MICROSOFT CORPORATION, APPELLANT

v.

UNITED STATES OF AMERICA, APPELLEE

Argued: Sept. 9, 2015
Decided: July 14, 2016

Before: LYNCH and CARNEY, *Circuit Judges*, and BOLDEN, *District Judge*.*

Microsoft Corporation appeals from orders of the United States District Court for the Southern District of New York (1) denying Microsoft's motion to quash a warrant ("Warrant") issued under the Stored Communications Act, 18 U.S.C. §§ 2701 *et seq.*, to the extent that the orders required Microsoft to produce the contents of a customer's email account stored on a server

---

* The Honorable Victor A. Bolden, of the United States District Court for the District of Connecticut, sitting by designation.

located outside the United States, and (2) holding Microsoft in civil contempt of court for its failure to comply with the Warrant. We conclude that § 2703 of the Stored Communications Act does not authorize courts to issue and enforce against U.S.-based service providers warrants for the seizure of customer e-mail content that is stored exclusively on foreign servers.

REVERSED, VACATED, AND REMANDED.

Judge Lynch concurs in a separate opinion.

SUSAN L. CARNEY, *Circuit Judge*:

Microsoft Corporation appeals from orders of the United States District Court for the Southern District of New York denying its motion to quash a warrant ("Warrant") issued under § 2703 of the Stored Communications Act ("SCA" or the "Act"), 18 U.S.C. §§ 2701 *et seq.*, and holding Microsoft in contempt of court for refusing to execute the Warrant on the government's behalf. The Warrant directed Microsoft to seize and produce the contents of an e-mail account that it maintains for a customer who uses the company's electronic communications services. A United States magistrate judge (Francis, *M.J.*) issued the Warrant on the government's application, having found probable cause to believe that the account was being used in furtherance of narcotics trafficking. The Warrant was then served on Microsoft at its headquarters in Redmond, Washington.

Microsoft produced its customer's non-content information to the government, as directed. That data was stored in the United States. But Microsoft ascertained that, to comply fully with the Warrant, it would need to access customer content that it stores and maintains in

Ireland and to import that data into the United States for delivery to federal authorities. It declined to do so. Instead, it moved to quash the Warrant. The magistrate judge, affirmed by the District Court (Preska, *C.J.*), denied the motion to quash and, in due course, the District Court held Microsoft in civil contempt for its failure.

Microsoft and the government dispute the nature and reach of the Warrant that the Act authorized and the extent of Microsoft's obligations under the instrument. For its part, Microsoft emphasizes Congress's use in the Act of the term "warrant" to identify the authorized instrument. Warrants traditionally carry territorial limitations: United States law enforcement officers may be directed by a court-issued warrant to seize items at locations in the United States and in United States-controlled areas, *see* Fed. R. Crim. P. 41(b), but their authority generally does not extend further.

The government, on the other hand, characterizes the dispute as merely about "compelled disclosure," regardless of the label appearing on the instrument. It maintains that "similar to a subpoena, [an SCA warrant] requir[es] the recipient to deliver records, physical objects, and other materials to the government" no matter where those documents are located, so long as they are subject to the recipient's custody or control. Gov't Br. at 6. It relies on a collection of court rulings construing properly-served subpoenas as imposing that broad obligation to produce without regard to a document's location. *E.g., Marc Rich & Co., A.G. v. United States*, 707 F.2d 663 (2d Cir. 1983).

For the reasons that follow, we think that Microsoft has the better of the argument. When, in 1986, Congress passed the Stored Communications Act as part of the broader Electronic Communications Privacy Act, its aim was to protect user privacy in the context of new technology that required a user's interaction with a service provider. Neither explicitly nor implicitly does the statute envision the application of its warrant provisions overseas. Three decades ago, international boundaries were not so routinely crossed as they are today, when service providers rely on worldwide networks of hardware to satisfy users' 21st-century demands for access and speed and their related, evolving expectations of privacy.

Rather, in keeping with the pressing needs of the day, Congress focused on providing basic safeguards for the privacy of domestic users. Accordingly, we think it employed the term "warrant" in the Act to require pre-disclosure scrutiny of the requested search and seizure by a neutral third party, and thereby to afford heightened privacy protection in the United States. It did not abandon the instrument's territorial limitations and other constitutional requirements. The application of the Act that the government proposes—interpreting "warrant" to require a service provider to retrieve material from beyond the borders of the United States—would require us to disregard the presumption against extraterritoriality that the Supreme Court re-stated and emphasized in *Morrison v. National Australian Bank Ltd.*, 561 U.S. 247 (2010) and, just recently, in *RJR Nabisco, Inc. v. European Cmty.*, 579 U.S. __, 2016 WL 3369423 (June 20, 2016). We are not at liberty to do so.

We therefore decide that the District Court lacked authority to enforce the Warrant against Microsoft. Because Microsoft has complied with the Warrant's domestic directives and resisted only its extraterritorial aspects, we REVERSE the District Court's denial of Microsoft's motion to quash, VACATE its finding of civil contempt, and REMAND the cause with instructions to the District Court to quash the Warrant insofar as it directs Microsoft to collect, import, and produce to the government customer content stored outside the United States.

BACKGROUND

I. Microsoft's Web-Based E-mail Service

The factual setting in which this dispute arose is largely undisputed and is established primarily by affidavits submitted by or on behalf of the parties.

Microsoft Corporation is a United States business incorporated and headquartered in Washington State. Since 1997, Microsoft has operated a "web-based e-mail" service available for public use without charge. Joint Appendix ("J.A.") at 35. It calls the most recent iteration of this service Outlook.com.[1] The service allows Microsoft customers to send and receive correspondence using e-mail accounts hosted by the company. In a protocol now broadly familiar to the ordinary citizen, a customer uses a computer to navigate to the Outlook.com web address, and there, after logging in with username and password, conducts correspondence electronically.

---

[1] The company inaugurated Outlook.com in 2013 as a successor to Microsoft's earlier Hotmail.com and MSN.com services.

Microsoft explains that, when it provides customers with web-based access to e-mail accounts, it stores the contents of each user's e-mails, along with a variety of non-content information related to the account and to the account's e-mail traffic, on a network of servers.[2] The company's servers are housed in datacenters operated by it and its subsidiaries.[3]

Microsoft currently makes "enterprise cloud service offerings" available to customers in over 100 countries through Microsoft's "public cloud."[4] The service offerings are "segmented into regions, and most customer data (*e.g.* email, calendar entries, and documents) is generally contained entirely within one or more data centers in the region in which the customer is located." J.A. at 109. Microsoft generally stores a customer's e-mail information and content at datacenters located near the physical location identified by the user as its own when subscribing to the service. Microsoft does

---

[2] A "server" is "a shared computer on a network that provides services to clients. . . . An Internet-connected web server is [a] common example of a server." Harry Newton & Steve Schoen, Newton's Telecom Dictionary 1084 (28th ed. 2014) ("*Newton's Telecom Dictionary*").

[3] A "datacenter" is "[a] centralized location where computing resources (*e.g.* host computers, servers, peripherals, applications, databases, and network access) critical to an organization are maintained in a highly controlled physical environment (temperature, humidity, etc.)." *Newton's Telecom Dictionary* at 373.

[4] The Supreme Court has recently described "[c]loud computing" as "the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself." *Riley v. California*, 134 S. Ct. 2473, 2491 (2014).

so, it explains, "in part to reduce 'network latency'"[5]—*i.e.*, delay—inherent in web-based computing services and thereby to improve the user's experience of its service. J.A. at 36-37. As of 2014, Microsoft "manage[d] over one million server computers in [its] datacenters worldwide, in over 100 discrete leased and owned datacenter facilities, spread over 40 countries." *Id.* at 109. These facilities, it avers, "host more than 200 online services, used by over 1 billion customers and over 20 million businesses worldwide." *Id.* at 109.

One of Microsoft's datacenters is located in Dublin, Ireland, where it is operated by a wholly owned Microsoft subsidiary. According to Microsoft, when its system automatically determines, "based on [the user's] country code," that storage for an e-mail account "should be migrated to the Dublin datacenter," it transfers the data associated with the account to that location. *Id.* at 37. Before making the transfer, it does not verify user identity or location; it simply takes the user-provided information at face value, and its systems migrate the data according to company protocol.

Under practices in place at the time of these proceedings, once the transfer is complete, Microsoft deletes from its U.S.-based servers "all content and non-content information associated with the account in the United States," retaining only three data sets in its U.S. facilities. *Id.* at 37. First, Microsoft stores some non-content e-mail information in a U.S.-located "data warehouse" that it operates "for testing and quality

---

[5] Microsoft explains network latency as "the principle of network architecture that the greater the geographical distance between a user and the datacenter where the user's data is stored, the slower the service." J.A. at 36.

control purposes." *Id.* Second, it may store some information about the user's online address book in a central "address book clearing house" that it maintains in the United States. Third, it may store some basic account information, including the user's name and country, in a U.S.-sited database. *Id.* at 37-38.

Microsoft asserts that, after the migration is complete, the "only way to access" user data stored in Dublin and associated with one of its customer's web-based e-mail accounts is "from the Dublin datacenter." *Id.* at 37. Although the assertion might be read to imply that a Microsoft employee must be physically present in Ireland to access the user data stored there, this is not so. Microsoft acknowledges that, by using a database management program that can be accessed at some of its offices in the United States, it can "collect" account data that is stored on any of its servers globally and bring that data into the United States. *Id.* at 39-40.

II. Procedural History

On December 4, 2013, Magistrate Judge James C. Francis IV of the United States District Court for the Southern District of New York issued the "Search and Seizure Warrant" that became the subject of Microsoft's motion to quash.

Although the Warrant was served on Microsoft, its printed boilerplate language advises that it is addressed to "[a]ny authorized law enforcement officer." *Id.* at 44. It commands the recipient to search "[t]he PREMISES known and described as the email account [redacted]@MSN.COM, which is controlled by Micro-

soft Corporation."[6] *Id.* It requires the "officer executing [the] warrant, or an officer present during the execution of the warrant" to "prepare an inventory . . . and promptly return [the] warrant and inventory to the Clerk of the Court." *Id.*

Its Attachment A, "Property To Be Searched," provides, "This warrant applies to information associated with [redacted]@msn.com, which is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation. . . . " *Id.* at 45. Attachment C, "Particular Things To Be Seized,"[7] directs Microsoft to disclose to the government, "for the period of inception of the account to the present," and "[t]o the extent that the information . . . is within the possession, custody, or control of MSN [redacted]," *id.*, the following information:

> (a) "The contents of all e-mails stored in the account, including copies of e-mails sent from the account";
>
> (b) "All records or other information regarding the identification of the account," including, among other things, the name, physical address, telephone numbers, session times and durations, log-in IP addresses, and sources of payment associated with the account;
>
> (c) "All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files"; and

---

[6] The name of the e-mail address associated with the account is subject to a sealing order and does not bear on our analysis.

[7] Although the Warrant includes an Attachment A and C, it appears to have no Attachment B.

> (d) "All records pertaining to communications between MSN [redacted] and any person regarding the account, including contacts with support services and records of actions taken."

J.A. 46-47.[8]

After being served with the Warrant, Microsoft determined that the e-mail contents stored in the account were located in its Dublin datacenter. Microsoft disclosed all other responsive information, which was kept within the United States, and moved the magistrate judge to quash the Warrant with respect to the user content stored in Dublin.

As we have recounted, the magistrate judge denied Microsoft's motion to quash. In a Memorandum and Order, he concluded that the SCA authorized the District Court to issue a warrant for "information that is stored on servers abroad." *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 15 F. Supp. 3d 466, 477 (S.D.N.Y. 2014) ("*In re Warrant*"). He observed that he had found probable cause for the requested search, and that the Warrant was properly served on Microsoft in the United States. He noted that, inasmuch as an SCA warrant is served on a service provider rather than on a law enforcement officer, it "is executed like a subpoena in that it . . . does not involve government agents entering the premises of the ISP [Internet service provider] to search its servers and seize the

---

[8] The Warrant also describes in Attachment C techniques that would be used (presumably by the government, not Microsoft) "to search the seized e-mails for evidence of the specified crime." J.A. at 47.

e-mail account in question." *Id.* at 471. Accordingly, he determined that Congress intended in the Act's warrant provisions to import obligations similar to those associated with a subpoena to "produce information in its possession, custody, or control regardless of the location of that information." *Id.* at 472 (citing *Marc Rich*, 707 F.2d at 667). While acknowledging that Microsoft's analysis in favor of quashing the Warrant with respect to foreign-stored customer content was "not inconsistent with the statutory language," he saw Microsoft's position as "undermined by the structure of the SCA, its legislative history," and "by the practical consequences that would flow from adopting it." He therefore concluded that Microsoft was obligated to produce the customer's content, wherever it might be stored. He also treated the place where the government would *review* the content (the United States), not the place of *storage* (Ireland), as the relevant place of seizure.

Microsoft appealed the magistrate judge's decision to Chief Judge Loretta A. Preska, who, on *de novo* review and after a hearing, adopted the magistrate judge's reasoning and affirmed his ruling from the bench. *In re Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 1:13-mj-02814 (S.D.N.Y. filed Dec. 4, 2013), ECF No. 80 (order reflecting ruling made at oral argument).

Microsoft timely noticed its appeal of the District Court's decision denying the motion to quash. Not long after, the District Court acted on a stipulation submitted jointly by the parties and held Microsoft in civil contempt for refusing to comply fully with the War-

rant.[9] *Id.* at ECF No. 92. Microsoft timely amended its notice of appeal to reflect its additional challenge to the District Court's contempt ruling.

We now reverse the District Court's denial of Microsoft's motion to quash; vacate the finding of contempt; and remand the case to the District Court with instructions to quash the Warrant insofar as it calls for production of customer content stored outside the United States.

III. Statutory Background

The Warrant was issued under the provisions of the Stored Communications Act, legislation enacted as Title II of the Electronic Communications Privacy Act of 1986. Before we begin our analysis, some background will be useful.

---

[9] As reflected in their stipulation, Microsoft and the government agreed to the contempt finding to ensure our Court's appellate jurisdiction over their dispute. *See United States v. Punn*, 737 F.3d 1, 5 (2d Cir. 2013) (noting general rule that contempt finding needed before ruling denying motion to quash is sufficiently "final" to support appellate jurisdiction). Because Microsoft timely appealed the contempt ruling, we need not decide whether we would have had jurisdiction over an appeal taken directly from the denial of the motion to quash. *See United States v. Constr. Prods. Research, Inc.*, 73 F.3d 464, 468-69 (2d Cir. 1996) (noting exception to contempt requirement as basis for appellate jurisdiction in context of third party subpoena issued in administrative investigation).

A. The Electronic Communications Privacy Act of 1986

The Electronic Communications Privacy Act ("ECPA") became law in 1986.[10] As it is summarized by the Department of Justice, ECPA "updated the Federal Wiretap Act of 1968, which addressed interception of conversations using 'hard' telephone lines, but did not apply to interception of computer and other digital and electronic communications."[11] ECPA's Title II is also called the Stored Communications Act ("SCA"). The Act "protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers," according to the Justice Department.[12] We discuss its provisions further below.

---

[10] Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1848, 1848-73 (1986) (codified as amended at 18 U.S.C. §§ 2510 *et seq.*, 18 U.S.C. §§ 2701 *et seq.*, and 18 U.S.C. §§ 3121 *et seq.*).

[11] U.S. Dep't of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Electronic Communications Privacy Act of 1986*, Justice Information Sharing, https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (last visited May 12, 2016). The Department advises that the acronym "ECPA" is commonly used to refer to the three titles of ECPA as a group (Titles I, II, and III of Pub. L. 99-508). *Id.* Title I "prohibits the intentional actual or attempted interception, use, disclosure, or procurement of any other person" to intercept wire, oral, or electronic transmissions; Title II is the Stored Communications Act, discussed in the text; Title III "addresses pen register and trap and trace devices," requiring government entities to obtain a court order authorizing their installation. *Id.* Title I and III are codified at 18 U.S.C. §§ 2510-22; Title II is codified at 18 U.S.C. §§ 2701-12, and constitutes chapter 121 of Title 18.

[12] *See supra* note 11.

B. The Technological Setting in 1986

When it passed the Stored Communications Act almost thirty years ago, Congress had as reference a technological context very different from today's Internet-saturated reality. This context affects our construction of the statute now.

One historian of the Internet has observed that "before 1988, the *New York Times* mentioned the Internet only once—in a brief aside." Roy Rosenzweig, *Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet*, 103 Am. Hist. Rev. 1530, 1530 (1998). The TCP/IP data transfer protocol—today, the standard for online communication—began to be used by the Department of Defense in about 1980. *See* Leonard Kleinrock, *An Early History of the Internet*, IEEE Commc'ns Mag. 26, 35 (Aug. 2010). The World Wide Web was not created until 1990, and we did not even begin calling it that until 1993. Daniel B. Garrie & Francis M. Allegra, *Plugged In: Guidebook to Software and the Law* § 3.2 (2015 ed.). Thus, a globally-connected Internet available to the general public for routine e-mail and other uses was still years in the future when Congress first took action to protect user privacy. *See* Craig Partridge, *The Technical Development of Internet Email*, IEEE Annals of the Hist. of Computing 3, 4 (Apr.-June 2008).

C. The Stored Communications Act

As the government has acknowledged in this litigation, "[t]he SCA was enacted to extend to electronic records privacy protections analogous to those provided by the Fourth Amendment." Gov't Br. at 29 (citing S. Comm. on Judiciary, Electronic Communications

Privacy Act of 1986, S. Rep. No. 99-541, at 5 (1986)). The SCA provides privacy protection for users of two types of electronic services—electronic communication services ("ECS") and remote computing services ("RCS")—then probably more distinguishable than now.[13] *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1213-14 (2004). An ECS generally operated by providing the user access to a central computer system through which to send electronic messages over telephone lines. S. Rep. No. 99-541, at 8. If the intended recipient also subscribed to the service, the provider temporarily stored the message in the recipient's electronic "mail box" until the recipient "call[ed] the company to retrieve its mail." *Id.* If the intended recipient was not a subscriber, the service provider could print the communication on paper and complete delivery by postal service or courier. *Id.*; U.S. Congress, Office of Technology Assessment, OTA-CIT-293, *Federal Government Information Technology: Electronic Surveillance and Civil Liberties* 47-48 (1985).[14] An RCS generally operated either by providing customers with access

---

[13] *See* 18 U.S.C. § 2510(15) (in ECPA Title I, defining "electronic communications service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications"); § 2711(2) (in ECPA Title II, the SCA, defining "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communications system").

[14] For example, in 1984, Federal Express entered the e-mail market with a service that provided for two-hour delivery of facsimile copies of e-mail messages up to five pages in length. U.S. Congress, Office of Technology Assessment, *Electronic Surveillance and Civil Liberties*, at 47.

to computer processing facilities in a "time-sharing arrangement," or by directly processing data that a customer transmitted electronically to the provider by means of electronic communications, and transmitting back the requested results of particular operations. S. Rep. No. 99-541, at 10-11. We will refer to Microsoft and other providers of ECS and RCS jointly as "service providers," except where the distinction makes a difference.

As to both services, the Act imposes general obligations of non-disclosure on service providers and creates several exceptions to those obligations. Thus, its initial provision, § 2701, prohibits unauthorized third parties from, among other things, obtaining or altering electronic communications stored by an ECS, and imposes criminal penalties for its violation. Section 2702 restricts the circumstances in which service providers may disclose information associated with and contents of stored communications to listed exceptions, such as with the consent of the originator or upon notice to the intended recipient, or pursuant to § 2703. Section 2703 then establishes conditions under which the government may require a service provider to disclose the contents of stored communications and related obligations to notify a customer whose material has been accessed. Section 2707 authorizes civil actions by entities aggrieved by violations of the Act, and makes "good faith reliance" on a court warrant or order "a complete defense." 18 U.S.C. § 2707(e).[15]

---

[15] Other provisions of the Act address, among other things, preservation of backup data (§ 2704); delaying notice to a customer whose information has been accessed (§ 2705); cost reimbursement for assembling data demanded under the Act (§ 2706); and exclu-

Regarding governmental access in particular, § 2703 sets up a pyramidal structure governing conditions under which service providers must disclose stored communications to the government. Basic subscriber and transactional information can be obtained simply with an administrative subpoena.[16] 18 U.S.C. § 2703(c)(2). Other non-content records can be obtained by a court order (a "§ 2703(d) order"), which may be issued only upon a statement of "specific and articulable facts showing . . . reasonable grounds to believe that the contents or records . . . are relevant and material to an ongoing criminal investigation." § 2703(c)(2), (d). The government may also obtain some user content with an administrative subpoena or a § 2703(d) order, but only if notice is provided to the service provider's subscriber or customer. § 2703(b)(1)(B). To obtain "priority stored communications" (our phrase), as described below, the Act generally requires that the government first secure a warrant that has been issued "using the procedures described in the Federal Rules of Criminal Procedure," or using State warrant procedures, both of which require a showing of probable cause.[17] Priority stored com-

---

sivity of remedies that the Act provides to a person aggrieved by its violation (§ 2708).

[16] An "administrative subpoena" is "a subpoena issued by an administrative agency to compel an individual to provide information to the agency." *Administrative subpoena*, Black's Law Dictionary (10th ed. 2014). To obtain such a subpoena, the government need not demonstrate probable cause. *See EEOC v. United Parcel Serv., Inc.*, 587 F.3d 136, 139-40 (2d Cir. 2009).

[17] Thus, § 2703, "Required disclosure of customer communications or records," provides in part as follows:

> (a) Contents of wire or electronic communications in electronic storage.—A governmental entity may require the disclosure by a provider of electronic communication service of the

contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communication system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title. . . .

(g) Presence of officer not required.—Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other

munications fall into two categories: For electronic communications stored *recently* (that is, for less than 180 days) by an ECS, the government *must* obtain a warrant. § 2703(a). For older electronic communications and those held by an RCS, a warrant is also required, unless the Government is willing to provide notice to the subscriber or customer. § 2703(b)(1)(A).

As noted, § 2703 calls for those warrants issued under its purview by federal courts to be "issued using the procedures described in the Federal Rules of Criminal Procedure." Rule 41 of the Federal Rules of Criminal Procedure, entitled "Search and Seizure," addresses federal warrants. It directs "the magistrate judge or a judge of a state court of record" to issue the warrant to "an officer authorized to execute it." Rule 41(e)(1). And insofar as territorial reach is concerned, Rule 41(b) describes the extent of the power of various authorities (primarily United States magistrate judges) to issue warrants with respect to persons or property located within a particular federal judicial district. It also allows magistrate judges to issue warrants that may be executed outside of the issuing district, but within another district of the United States. Fed. R. Crim. P. 41(b)(2), (b)(3). Rule 41(b)(5) generally restricts the geographical reach of a warrant's execution, if not in another federal district, to "a United States territory, possession, or commonwealth," and various diplomatic or consular missions of the United States or diplomatic residences of the United States located in a foreign state.

---

information pertaining to a subscriber to or customer of such service.

DISCUSSION

I. Standard of Review

We will vacate a finding of civil contempt that rests on a party's refusal to comply with a court order if we determine that the district court relied on a mistaken understanding of the law in issuing its order. *United States ex rel. Touhy v. Ragen*, 340 U.S. 462, 464-70 (1951). Similarly, we will vacate a district court's denial of a motion to quash if we conclude that the denial rested on a mistake of law.[18] *See In re Subpoena Issued to Dennis Friedman*, 350 F.3d 65, 68-69 (2d Cir. 2003).

It is on the legal predicate for the District Court's rulings—its analysis of the Stored Communications Act, in particular, and of the principles of construction set forth by the Supreme Court in *Morrison v. National Australian Bank Ltd.*, 561 U.S. 247 (2010) —that we focus our attention in this appeal.

II. Whether the SCA Authorizes Enforcement of the Warrant as to Customer Content Stored in Ireland

A. Analytic Framework

The parties stand far apart in the analytic frameworks that they present as governing this case.

Adopting the government's view, the magistrate judge denied Microsoft's motion to quash, resting on

---

[18] Our Court has not squarely held what standard governs our review of a district court's denial of a motion to quash and its related contempt finding. We need not dwell long on this threshold question, however, because even a deferential abuse-of-discretion review incorporates a *de novo* examination of the district court's rulings of law, such as we conduct here. *See, e.g., In re Grand Jury Subpoena Issued June 18, 2009*, 593 F.3d 155, 157 (2d Cir. 2010).

the legal conclusion that an SCA warrant is more akin to a subpoena than a warrant, and that a properly served subpoena would compel production of any material, including customer content, so long as it is stored at premises "owned, maintained, controlled, or operated by Microsoft Corporation." *In re Warrant*, 15 F. Supp. 3d at 468 (quoting Warrant). The fact that those premises were located abroad was, in the magistrate judge's view, of no moment. *Id.* at 472.

Microsoft offers a different conception of the reach of an SCA warrant. It understands such a warrant as more closely resembling a traditional warrant than a subpoena. In its view, a warrant issued under the Act cannot be given effect as to materials stored beyond United States borders, regardless of what may be retrieved electronically from the United States and where the data would be reviewed. To enforce the Warrant as the government proposes would effect an unlawful extraterritorial application of the SCA, it asserts, and would work an unlawful intrusion on the privacy of Microsoft's customer.

Although electronic data may be more mobile, and may seem less concrete, than many materials ordinarily subject to warrants, no party disputes that the electronic data subject to this Warrant were in fact located in Ireland when the Warrant was served. None disputes that Microsoft would have to collect the data from Ireland to provide it to the government in the United States. As to the citizenship of the customer whose e-mail content was sought, the record is silent. For its part, the SCA is silent as to the reach of the statute as a whole and as to the reach of its warrant provisions in particular. Finally, the presumption against extrater-

ritorial application of United States statutes is strong and binding. *See Morrison*, 561 U.S. at 255. In these circumstances, we believe we must begin our analysis with an inquiry into whether Congress, in enacting the warrant provisions of the SCA, envisioned and intended those provisions to reach outside of the United States. If we discern that it did not, we must assess whether the enforcement of this Warrant constitutes an unlawful extraterritorial application of the statute. We thus begin with a brief review of *Morrison*, which outlines the operative principles.

B. *Morrison* and the Presumption Against Extraterritoriality

When interpreting the laws of the United States, we presume that legislation of Congress "is meant to apply only within the territorial jurisdiction of the United States," unless a contrary intent clearly appears. *Id.* at 255 (internal quotation marks omitted); *see also RJR Nabisco, Inc. v. European Cmty.*, 579 U.S. __, __, 2016 WL 3369423, at *7 (June 20, 2016). This presumption rests on the perception that "Congress ordinarily legislates with respect to domestic, not foreign matters." *Id.* The presumption reflects that Congress, rather than the courts, has the "facilities necessary" to make policy decisions in the "delicate field of international relations." *Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013) (quoting *Benz v. Compania Naviera Hidalgo, S.A.*, 353 U.S. 138, 147 (1957)). In line with this recognition, the presumption is applied to protect against "unintended clashes between our laws and those of other nations which could result in international discord." *Equal Emp't Opportunity Comm'n v. Arabian American Oil Co.*, 499 U.S. 244, 248 (1991)

("*Aramco*"); *see generally Park Central Global Hub Ltd. v. Porsche Auto. Holdings SE*, 763 F.3d 198 (2d Cir. 2014) (per curiam).

To decide whether the presumption limits the reach of a statutory provision in a particular case, "we look to see whether 'language in the [relevant Act] gives any indication of a congressional purpose to extend its coverage beyond places over which the United States has sovereignty or has some measure of legislative control.'" *Aramco*, 499 U.S. at 248 (alteration in original) (quoting *Foley Bros., Inc. v. Filardo*, 336 U.S. 281, 285 (1949)). The statutory provision must contain a "clear indication of an extraterritorial application"; otherwise, "it has none." *Morrison*, 561 U.S. at 255; *see also RJR Nabisco*, 579 U.S. at __, 2016 WL 3369423, at *7.

Following the approach set forth in *Morrison*, our inquiry proceeds in two parts. We first determine whether the relevant statutory provisions contemplate extraterritorial application. *Id.* at 261-65. If we conclude that they do not, by identifying the statute's focus and looking at the facts presented through that prism, we then assess whether the challenged application is "extraterritorial" and therefore outside the statutory bounds. *Id.* at 266-70.

C. Whether the SCA's Warrant Provisions Contemplate Extraterritorial Application

We dispose of the first question with relative ease. The government conceded at oral argument that the warrant provisions of the SCA do not contemplate or

permit extraterritorial application.[19] Our review of the statute confirms the soundness of this concession.

1. Plain Meaning of the SCA

As observed above, the SCA permits the government to require service providers to produce the contents of certain priority stored communications "only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction." 18 U.S.C. § 2703(a), (b)(1)(a). The provisions in § 2703 that permit a service provider's disclosure in response to a duly obtained warrant do not mention any extraterritorial application, and the government points to no provision that even implicitly alludes to any such application. No relevant definition provided by either Title I or Title II of ECPA, *see* 18 U.S.C. §§ 2510, 2711, suggests that Congress envisioned any extraterritorial use for the statute.

When Congress intends a law to apply extraterritorially, it gives an "affirmative indication" of that intent. *Morrison*, 561 U.S. at 265. It did so, for example, in

---

[19] When asked, "What text in the Stored Communications Act do you point to, to support your assertion that . . . Congress intended extraterritorial application?", the government responded, "There's no extraterritorial application here at all." Recording of Oral Argument at 1:06:40-1:07:00. Later, when Judge Lynch observed, "I take it that suggests that the government actually agrees that there shall not be extraterritorial application of the Stored Communications Act . . . what this dispute is about is about the focus of the statute and what counts as an extraterritorial application of the statute," the government answered, "That's right, Judge." *Id.* at 1:25:38-1:26:05.

the statutes at issue in *Weiss v. National Westminster Bank PLC*, 768 F.3d 202, 207 & n.5 (2d Cir. 2014) (concluding that definition of "international terrorism" within 18 U.S.C. § 2331(1) covers extraterritorial conduct because Congress referred to acts that "occur primarily outside the territorial jurisdiction of the United States") and *United States v. Weingarten*, 632 F.3d 60, 65 (2d Cir. 2011) (concluding that 18 U.S.C. § 2423(b) applies to extraterritorial conduct because it criminalizes "travel in foreign commerce undertaken with the intent to commit sexual acts with minors" that would violate United States law had the acts occurred in the jurisdiction of the United States). We see no such indication in the SCA.

We emphasize further that under § 2703, any "court of competent jurisdiction"—defined in § 2711(3)(B) to include "a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants"—may issue an SCA warrant. Section 2703(a) refers directly to the use of State warrant procedures as an adequate basis for issuance of an SCA warrant. 18 U.S.C. § 2703(a). We think it particularly unlikely that, if Congress intended SCA warrants to apply extraterritorially, it would provide for such far-reaching state court authority without at least "address[ing] the subject of conflicts with foreign laws and procedures." *Aramco*, 499 U.S. at 256; *see also American Ins. Ass'n v. Garamendi*, 539 U.S. 396, 413 (2003) (describing as beyond dispute the notion that "state power that touches on foreign relations must yield to the National Government's policy").

The government asserts that "[n]othing in the SCA's text, structure, purpose, or legislative history indicates

that compelled production of records is *limited* to those stored domestically." Gov't Br. at 26 (formatting altered and emphasis added). It emphasizes the requirement placed on a service provider to disclose customers' data, and the absence of any territorial reference restricting that obligation. We find this argument unpersuasive: It stands the presumption against extraterritoriality on its head. It further reads into the Act an extraterritorial awareness and intention that strike us as anachronistic, and for which we see, and the government points to, no textual or documentary support.[20]

2. The SCA's Use of the Term of Art "Warrant"

Congress's use of the term of art "warrant" also emphasizes the domestic boundaries of the Act in these circumstances.

In construing statutes, we interpret a legal term of art in accordance with the term's traditional legal meaning, unless the statute contains a persuasive indication that Congress intended otherwise. *See F.A.A. v. Cooper*, 132 S. Ct. 1441, 1449 (2012) ("[W]hen Congress employs a term of art, 'it presumably knows and adopts the cluster of ideas that were attached to each borrowed word in the body of learning from which it was

---

[20] Seeking additional grounds for its position that to apply *Morrison* in this case is to proceed on a false premise, the government argues that the presumption against extraterritoriality applies only to "substantive provisions" of United States law, and that the SCA's warrant provisions are procedural. Gov't Br. at 31. The proposition that the SCA's protections are merely procedural might reasonably be questioned. But even assuming that they are procedural, the government gains no traction with this argument, which we rejected in *Loginovskaya v. Batratchenko*, 764 F.3d 266, 272-73 (2d Cir. 2014).

taken.'") (quoting *Molzof v. United States*, 502 U.S. 301, 307 (1992)). "Warrant" is such a term of art.

The term is endowed with a legal lineage that is centuries old. The importance of the warrant as an instrument by which the power of government is exercised and constrained is reflected by its prominent appearance in the Fourth Amendment to the United States Constitution:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. It is often observed that "[t]he chief evil that prompted the framing and adoption of the Fourth Amendment was the indiscriminate searches and seizures conducted by the British under the authority of general warrants." *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (internal quotation marks omitted). Warrants issued in accordance with the Fourth Amendment thus identify discrete objects and places, and restrict the government's ability to act beyond the warrant's purview—of particular note here, outside of the place identified, which must be described in the document. *Id.* at 445-46.

As the term is used in the Constitution, a warrant is traditionally moored to privacy concepts applied within the territory of the United States: "What we know of the history of the drafting of the Fourth Amendment . . . suggests that its purpose was to restrict searches

and seizures which might be conducted by the United States in domestic matters." *In re Terrorist Bombings of U.S. Embassies in East Africa*, 552 F.3d 157, 169 (2d Cir. 2008) (alteration omitted and ellipses in original) (quoting *United States v. Verdugo-Urquidez*, 494 U.S. 259, 266 (1990)). Indeed, "if U.S. judicial officers were to issue search warrants intended to have extraterritorial effect, such warrants would have dubious legal significance, if any, in a foreign nation." *Id.* at 171. Accordingly, a warrant protects privacy in a distinctly territorial way.[21]

The SCA's legislative history related to its post enactment amendments supports our conclusion that Congress intended to invoke the term "warrant" with all of its traditional, domestic connotations.[22] Since the SCA's initial passage in 1986, Congress has amended § 2703 to relax some of the Rule 41 requirements as they relate to SCA warrants. Although some address the

---

[21] The government argues that the SCA's warrant provisions were "modeled after the Right to Financial Privacy Act," 12 U.S.C. §§ 3402(3), 3406, and that the latter act also "envisions that warrants —along with subpoenas and summonses—will trigger a disclosure requirement." Gov't Br. at 19 (citing S. Rep. No. 99-541, at 3). It points to no authority definitively construing the latter act's warrant provisions, however, nor any acknowledgment in the history of the SCA that enforcement of the warrant's disclosure commands would cross international boundaries. For these reasons, we accord little weight to the observation.

[22] We note that a 2009 amendment to Rule 41 expressly authorizes the use of such warrants to seize electronically-stored data, without abandoning the requirement that the warrant specify the place from which the data is to be seized. *See* Fed. R. Crim. P. 41(e)(2)(B) (allowing magistrate judge to "authorize the seizure of *electronic storage media* or the seizure or copying of *electronically stored information*" (emphasis added)).

reach of SCA warrants, none of the amendments contradicts the term's traditional domestic limits. *See* USA PATRIOT ACT, Pub. L. 107-56, § 220; 115 Stat. 272, 291-92 (2001) (codified at 18 U.S.C.§ 2703(a), (b)); 21st Century Department of Justice Appropriations Authorization Act, Pub. L. 107-273, § 11010, 116 Stat. 1758, 1822 (2002) (codified at 18 U.S.C. § 2703(g)); Foreign Evidence Request Efficiency Act of 2009, Pub. L. 111-79, § 2, 123 Stat. 2086, 2086 (2009) (codified at 18 U.S.C. § 2711(3)(A)). These amendments to the SCA are fully consistent with the historical role of warrants as legal instruments that pertain to discrete objects located within the United States, and that are designed to protect U.S. citizens' privacy interests.

The magistrate judge took a different view of the legislative history of certain amendments to the SCA. He took special notice of certain legislative history related to the 2001 amendment to the warrant provisions enacted in the USA PATRIOT ACT. A House committee report explained that "[c]urrently, Federal Rules [*sic*] of Criminal Procedure 41 requires that the 'warrant' be obtained 'within the district' where the property is located. An investigator, for example, located in Boston . . . might have to seek a suspect's electronic e-mail from an Internet service provider (ISP) account located in California." *In re Warrant*, 15 F. Supp. 3d at 473 (quoting H.R. Rep. 107-236(I), at 57 (2001)). The magistrate judge reasoned that this statement equated the location of property with the location of the service provider, and not with the location of any server. *Id.* at 474.

But this excerpt says nothing about the need to cross international boundaries; rather, while noting the

"cross-jurisdictional nature of the Internet," it discusses only amendments to Rule 41 that allow magistrate judges "within the district" to issue warrants to be executed in other "districts"—not overseas. *Id.* at 473 (quoting H.R. Rep. 107-236(I), at 58). Furthermore, the Committee discussion reflects no expectation that the material to be searched and seized would be located any place other than where the service provider is located. Thus, the Committee's hypothetical focuses on a situation in which an investigator in Boston might seek e-mail from "an Internet service provider (ISP) *account* located in California." To our reading, the Report presumes that the service provider is located where the account is—within the United States.[23]

3. Relevance of Law on "Subpoenas"

We reject the approach, urged by the government and endorsed by the District Court, that would treat the SCA warrant as equivalent to a subpoena. The District Court characterized an SCA warrant as a "hybrid" between a traditional warrant and a subpoena because —generally unlike a warrant—it is executed by a service provider rather than a government law enforcement agent, and because it does not require the pres-

---

[23] Our brief discussion here of the law of warrants is offered in aid only of our interpretation of the statutory language. Consequently, we do not consider whether the Fourth Amendment might be understood to impose disclosure-related procedural requirements more stringent than those established by the SCA. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (finding Fourth Amendment protects certain electronic communications based on users' reasonable expectations of privacy); *see also* Email Privacy Act, H. R. 699, 114th Cong. § 3 (passed by House Apr. 27, 2016) (requiring government to obtain warrant before obtaining documents stored online).

ence of an agent during its execution. *Id.* at 471; 18 U.S.C. § 2703(a)-(c), (g). As flagged earlier, the subpoena-warrant distinction is significant here because, unlike warrants, subpoenas may require the production of communications stored overseas. 15 F. Supp. 3d at 472 (citing *Marc Rich*, 707 F.2d at 667).

Warrants and subpoenas are, and have long been, distinct legal instruments.[24] Section 2703 of the SCA recognizes this distinction and, unsurprisingly, uses the "warrant" requirement to signal (and to provide) a greater level of protection to priority stored communications, and "subpoenas" to signal (and provide) a lesser level. 18 U.S.C. § 2703(a), (b)(1)(A). Section 2703 does not use the terms interchangeably. *Id.* Nor does it use the word "hybrid" to describe an SCA warrant. Indeed, § 2703 places priority stored communications entirely outside the reach of an SCA subpoena, absent compliance with the notice provisions. *Id.* The term "subpoena," therefore, stands separately in the statute, as in ordinary usage, from the term "warrant." We see no reasonable basis in the

---

[24] A "subpoena" (from the Latin phrase meaning "under penalty,") is "[a] writ or order commanding a person to appear before a court or other tribunal, subject to a penalty for failing to comply." *Subpoena*, Black's Law Dictionary. Relatedly, a "subpoena duces tecum" directs the person served to bring with him "specified documents, records, or things." *Subpoena duces tecum*, Black's Law Dictionary. In contrast, a "warrant" is a "writ directing or authorizing someone to do an act [such as] one directing a law enforcer to make . . . a search, or a seizure." *Warrant*, Black's Law Dictionary. As to search warrants, the place is key: A search warrant is a "written order authorizing a law-enforcement officer to conduct a search *of a specified place*." *Search Warrant*, Black's Law Dictionary.

statute from which to infer that Congress used "warrant" to mean "subpoena."

Furthermore, contrary to the Government's assertion, the law of warrants has long contemplated that a private party may be required to participate in the lawful search or seizure of items belonging to the target of an investigation. When the government compels a private party to assist it in conducting a search or seizure, the private party becomes an agent of the government, and the Fourth Amendment's warrant clause applies in full force to the private party's actions. *See Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971); *Gambino v. United States*, 275 U.S. 310, 316-17 (1927); *see also Cassidy v. Chertoff*, 471 F.3d 67, 74 (2d Cir. 2006). The SCA's warrant provisions fit comfortably within this scheme by requiring a warrant for the content of stored communications even when the warrant commands a service provider, rather than a law enforcement officer, to access the communications. 18 U.S.C. § 2703(a), (b)(1)(A), (g). Use of this mechanism does not signal that, notwithstanding its use of the term "warrant," Congress intended the SCA warrant procedure to function like a traditional subpoena. We see no reason to believe that Congress intended to jettison the centuries of law requiring the issuance and performance of warrants in specified, domestic locations, or to replace the traditional warrant with a novel instrument of international application.

The government nonetheless urges that the law of subpoenas relied on by the magistrate judge requires a subpoena's recipient to produce documents no matter where located, and that this aspect of subpoena law should be imported into the SCA's warrant provisions.

The government argues that "subpoenas, orders, and warrants are equally empowered to obtain records . . . through a disclosure requirement directed at a service provider." Gov't Br. at 18-19. It further argues that disclosure in response to an SCA warrant should not be read to reach only U.S.-located documents, but rather all records available to the recipient. *Id.* at 26-27.

In this, the government rests on our 1983 decision in *Marc Rich*. There, we permitted a grand jury subpoena issued in a tax evasion investigation to reach the overseas business records of a defendant Swiss commodities trading corporation. The *Marc Rich* Court clarified that a defendant subject to the personal jurisdiction of a subpoena-issuing grand jury could not "resist the production of [subpoenaed] documents on the ground that the documents are located abroad." 707 F.2d at 667. The federal court had subject-matter jurisdiction over the foreign defendant's actions pursuant to the "territorial principle," which allows governments to punish an individual for acts outside their boundaries when those acts are "intended to produce and do produce detrimental effects within it." *Id.* at 666. In investigating such a case, the Court concluded, the grand jury necessarily had authority to obtain evidence related to the foreign conduct, even when that evidence was located abroad. *Id.* at 667. For that reason, as long as the Swiss corporation was subject to the grand jury's personal jurisdiction—which the Court concluded was the case—the corporation was bound by its subpoena. *Id.* Thus, in *Marc Rich*, a subpoena could reach documents located abroad when the subpoenaed foreign defendant was being compelled to turn over its

own records regarding potential illegal conduct, the effects of which were felt in the United States.

Contrary to the government's assertion, neither *Marc Rich* nor the statute gives any firm basis for importing law developed in the subpoena context into the SCA's warrant provisions. Microsoft convincingly observes that our Court has never upheld the use of a subpoena to compel a recipient to produce an item under its control and located overseas when the recipient is merely a caretaker for another individual or entity and that individual, not the subpoena recipient, has a protectable privacy interest in the item.[25] Appellant's Br. at 42-43. The government does not identify, and our review of this Court's precedent does not reveal, any such cases.

The government also cites, and the District Court relied on, a series of cases in which banks have been required to comply with subpoenas or discovery orders

---

[25] The government contends that Microsoft has waived the argument that the government cannot compel production of records that Microsoft holds on its customers' behalf. Gov't Br. at 36 & n.14. But in the District Court proceedings, Microsoft argued that there was a "difference between, on the one hand asking a company for its own documents . . . versus when you are going after someone else's documents . . . that are entrusted to us on behalf of our clients." Transcript of Oral Argument at 17, *In re Warrant*, 1:13-mj-02814, ECF No. 93. Although this was not the centerpiece of Microsoft's argument before the District Court, it was sufficiently raised. And in any event, we are free to consider arguments made on appeal in the interests of justice even when they were not raised before the district court. *See Gibeau v. Nellis*, 18 F.3d 107, 109 (2d Cir. 1994). The government has had an ample opportunity to rebut Microsoft's position, and we see no reason to treat this important argument as beyond our consideration.

requiring disclosure of their overseas records, notwithstanding the possibility that compliance would conflict with their obligations under foreign law.[28] But the Supreme Court has held that bank depositors have no protectable privacy interests in a bank's records regarding their accounts. *See United States v. Miller*, 425 U.S. 435, 440-41 (1976) (explaining that the records a bank creates from the transactions of its depositors are the bank's "business records" and not its depositors' "private papers"). Thus, our 1968 decision in *United States v. First National City Bank* poses no bar to Microsoft's argument. There, we held that a bank subject to the jurisdiction of a federal court was not absolutely entitled to withhold from a grand jury subpoena its banking records held in Frankfurt, Germany "relating to any transaction in the name of (or for the benefit of)" certain foreign customers solely because the bank faced the prospect of civil liability. 396 F.2d 897, 898, 901, 905 (2d Cir. 1968); *cf. Linde v. Arab Bank, PLC*, 706 F.3d 92, 101-02, 109 (2d Cir. 2013) (declining to issue writ of mandamus overturning district court's imposition of sanctions on foreign bank, when bank was civil defendant and refused to comply with discovery orders seeking certain foreign banking records).

---

[28] Thus, in addition to *Marc Rich*, the government refers us to other cases that it characterizes as ordering production despite potential or certain conflict with the laws of other nations: *In re Grand Jury Proceedings (Bank of Nova Scotia)*, 740 F.2d 817, 826-29 (11th Cir. 1984); *United States* v. *Vetco Inc.*, 691 F.2d 1281, 1287-91 (9th Cir. 1981); *In re Grand Jury Subpoena Dated August 9, 2000*, 218 F. Supp. 2d 544, 547, 554 (S.D.N.Y. 2002) (Chin, J.); *United States* v. *Chase Manhattan Bank, N.A.*, 584 F. Supp. 1080, 1086-87 (S.D.N.Y. 1984). Gov't Br. at 16-17.

We therefore conclude that Congress did not intend the SCA's warrant provisions to apply extraterritorially.

D. Discerning the "Focus" of the SCA

This conclusion does not resolve the merits of this appeal, however, because "it is a rare case of prohibited extraterritorial application that lacks *all* contact with the territory of the United States." *Morrison*, 561 U.S. at 266. When we find that a law does not contemplate or permit extraterritorial application, we generally must then determine whether the case at issue involves such a prohibited application. *Id* at 266-67. As we recently observed in *Mastafa v. Chevron Corp.*, "An evaluation of the presumption's application to a particular case is essentially an inquiry into whether the domestic contacts are sufficient to avoid triggering the presumption at all." 770 F.3d 170, 182 (2d Cir. 2014).

In making this second-stage determination, we first look to the "territorial events or relationships" that are the "focus" of the relevant statutory provision. *Id.* at 183 (alterations and internal quotation marks omitted). If the domestic contacts presented by the case fall within the "focus" of the statutory provision or are "the objects of the statute's solicitude," then the application of the provision is not unlawfully extraterritorial. *Morrison*, 561 U.S. at 267. If the domestic contacts are merely secondary, however, to the statutory "focus," then the provision's application to the case is extraterritorial and precluded.

In identifying the "focus" of the SCA's warrant provisions, it is helpful to resort to the familiar tools of statutory interpretation, considering the text and plain meaning of the statute, *see, e.g., Gottlieb v. Carnival*

Corp., 436 F.3d 335, 337 (2d Cir. 2006), as well as its framework, procedural aspects, and legislative history. *Cf. Morrison*, 561 U.S. at 266-70 (looking to text and statutory context to discern focus of statutory provision); *Loginovskaya*, 764 F.3d at 272-73 (analyzing text, context, and precedent to discern focus for *Morrison* purposes). Having done so, we conclude that the relevant provisions of the SCA focus on protecting the privacy of the content of a user's stored electronic communications. Although the SCA also prescribes methods under which the government may obtain access to that content for law enforcement purposes, it does so in the context of a primary emphasis on protecting user content—the "object[] of the statute's solicitude." *Morrison*, 561 U.S. at 267.

1. The SCA's Warrant Provisions

The reader will recall the SCA's provisions regarding the production of electronic communication content: In sum, for priority stored communications, "a governmental entity may require the disclosure . . . of the contents of a wire or electronic communication . . . only pursuant to a warrant issued using the rules described in the Federal Rules of Criminal Procedure," except (in certain cases) if notice is given to the user. 18 U.S.C. § 2703(a), (b).

In our view, the most natural reading of this language in the context of the Act suggests a legislative focus on the privacy of stored communications. Warrants under § 2703 must issue under the Federal Rules of Criminal Procedure, whose Rule 41 is undergirded by the Constitution's protections of citizens' privacy against unlawful searches and seizures. And more generally, § 2703's warrant language appears in a statute

entitled the Electronic Communications Privacy Act, suggesting privacy as a key concern.

The overall effect is the embodiment of an expectation of privacy in those communications, notwithstanding the role of service providers in their transmission and storage, and the imposition of procedural restrictions on the government's (and other third party) access to priority stored communications. The circumstances in which the communications have been stored serve as a proxy for the intensity of the user's privacy interests, dictating the stringency of the procedural protection they receive—in particular whether the Act's warrant provisions, subpoena provisions, or its § 2703(d) court order provisions govern a disclosure desired by the government. Accordingly, we think it fair to conclude based on the plain meaning of the text that the privacy of the stored communications is the "object[] of the statute's solicitude," and the focus of its provisions. *Morrison*, 561 U.S. at 267.

2. Other Aspects of the Statute

In addition to the text's plain meaning, other aspects of the statute confirm its focus on privacy.

As we have noted, the first three sections of the SCA contain its major substantive provisions. These sections recognize that users of electronic communications and remote computing services hold a privacy interest in their stored electronic communications. In particular, § 2701(a) makes it unlawful to "intentionally access[] without authorization," or "intentionally exceed[] an authorization to access," a "facility through which an electronic communication service is provided" and "thereby obtain[], alter[], or prevent[] authorized access

to a wire or electronic communication while it is in electronic storage." Contrary to the government's contention, this section does more than merely protect against the disclosure of information by third parties. By prohibiting the alteration or blocking of access to stored communications, this section also shelters the communications' integrity. Section 2701 thus protects the privacy interests of users in many aspects of their stored communications from intrusion by unauthorized third parties.

Section 2702 generally prohibits providers from "knowingly divulg[ing]" the "contents" of a communication that is in electronic storage subject to certain enumerated exceptions. 18 U.S.C. § 2702(a). Sections 2701 and 2702 are linked by their parallel protections for communications that are in electronic storage. Section 2703 governs the circumstances in which information associated with stored communications may be disclosed to the government, creating the elaborate hierarchy of privacy protections that we have described.

From this statutory framework we find further reason to conclude that the SCA's focus lies primarily on the need to protect users' privacy interests. The primary obligations created by the SCA protect the electronic communications. Disclosure is permitted only as an exception to those primary obligations and is subject to conditions imposed in § 2703. Had the Act instead created, for example, a rebuttable presumption of law enforcement access to content premised on a minimal showing of legitimate interest, the government's argument that the Act's focus is on aiding law enforcement and disclosure would be stronger. *Cf.*

Morrison, 561 U.S. at 267. But this is not what the Act does.

The SCA's procedural provisions further support our conclusion that the Act focuses on user privacy. As noted above, the SCA expressly adopts the procedures set forth in the Federal Rules of Criminal Procedure. 18 U.S.C. § 2703(a), (b)(1)(A). Rule 41, which governs the issuance of warrants, reflects the historical understanding of a warrant as an instrument protective of the citizenry's privacy. *See* Fed. R. Crim. P. 41. Further, the Act provides criminal penalties for breaches of those privacy interests and creates civil remedies for individuals aggrieved by a breach of their privacy that violates the Act. *See* 18 U.S.C. §§ 2701, 2707. These all buttress our sense of the Act's focus.

We find unpersuasive the government's argument, alluded to above, that the SCA's warrant provisions must be read to focus on "disclosure" rather than privacy because the SCA permits the government to obtain by mere subpoena the content of e-mails that have been held in ECS storage for *more than* 180 days. Gov't Br. at 28-29; *see* 18 U.S.C. § 2703(a). In this vein, the government submits that reading the SCA's warrant provisions to focus on the privacy of stored communications instead of disclosure would anomalously place newer e-mail content stored on foreign servers "beyond the reach of the statute entirely," while older e-mail content stored on foreign servers could be obtained simply by subpoena, if notice is given to the user. Gov't Br. at 29. This argument assumes, however, that a subpoena issued to Microsoft under the SCA's subpoena provisions would reach a user's e-mail content stored on foreign servers. Although our Court's

precedent regarding the foreign reach of subpoenas (and *Marc Rich* in particular) might suggest this result, the protections rightly accorded user content in the face of an SCA subpoena have yet to be delineated. Today, we need not determine the reach of the SCA's subpoena provisions, because we are faced here only with the lawful reach of an SCA warrant. Certainly, the service provider's role in relation to a customer's content supports the idea that persuasive distinctions might be drawn between it and other categories of subpoena recipients. *See supra* note 23.

In light of the plain meaning of the statutory language and the characteristics of other aspects of the statute, we conclude that its privacy focus is unmistakable.

3. Legislative History

We consult the Act's legislative history to test our conclusion.

In enacting the SCA, Congress expressed a concern that developments in technology could erode the privacy interest that Americans traditionally enjoyed in their records and communications. *See* S. Rep. No. 99-541, at 3 ("With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information."); H.R. Rep. No. 99-647, at 19 (1986) ("[M]ost important, if Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right."). In particular, Congress noted that the actions of private parties were largely unregulated when it came to maintaining the privacy of stored electronic communications. *See* S. Rep. No. 99-541, at 3;

H.R. Rep. No. 99-647, at 18. And Congress observed further that recent Supreme Court precedent called into question the breadth of the protection to which electronic records and communications might be entitled under the Fourth Amendment. *See* S. Rep. No. 99-541, at 3 (citing *United States v. Miller*, 425 U.S. 435 (1976), for proposition that because records and private correspondence in computing context are "subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection"); H.R. Rep. No. 99-647, at 23 (citing *Miller* for proposition that "under current law a subscriber or customer probably has very limited rights to assert in connection with the disclosure of records held or maintained by remote computing services").

Accordingly, Congress set out to erect a set of statutory protections for stored electronic communications. *See* S. Rep. No. 99-541, at 3; H.R. Rep. No. 99-647, at 19. In regard to governmental access, Congress sought to ensure that the protections traditionally afforded by the Fourth Amendment extended to the electronic forum. *See* H.R. Rep. No. 99-647, at 19 ("Additional legal protection is necessary to ensure the continued vitality of the Fourth Amendment."). It therefore modeled § 2703 after its understanding of the scope of the Fourth Amendment. As the House Judiciary Committee explained in its report, it appeared likely to the Committee that "the courts would find that the parties to an e-mail transmission have a 'reasonable expectation of privacy' and that a warrant of some kind is required." *Id.* at 22.

We believe this legislative history tends to confirm our view that the Act's privacy provisions were its

impetus and focus. Although Congress did not overlook law enforcement needs in formulating the statute, neither were those needs the primary motivator for the enactment. *See* S. Rep. No. 99-541, at 3 (in drafting SCA, Senate Judiciary Committee sought "to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs").

Taken as a whole, the legislative history tends to confirm our view that the focus of the SCA's warrant provisions is on protecting users' privacy interests in stored communications.

E. Extraterritoriality of the Warrant

Having thus determined that the Act focuses on user privacy, we have little trouble concluding that execution of the Warrant would constitute an unlawful extraterritorial application of the Act. *See Morrison*, 561 U.S. at 266-67; *RJR Nabisco*, 579 U.S. at __, 2016 WL 3369423, at *9.

The information sought in this case is the content of the electronic communications of a Microsoft customer. The content to be seized is stored in Dublin. J.A. at 38. The record is silent regarding the citizenship and location of the customer. Although the Act's focus on the customer's privacy might suggest that the customer's actual location or citizenship would be important to the extraterritoriality analysis, it is our view that the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed —here, where it is seized by Microsoft, acting as an

agent of the government.[27] Because the content subject to the Warrant is located in, and would be seized from, the Dublin datacenter, the conduct that falls within the focus of the SCA would occur outside the United States, regardless of the customer's location and regardless of Microsoft's home in the United States.[28] *Cf. Riley v. California*, 134 S. Ct. 2473, 2491 (2014) (noting privacy concern triggered by possibility that search of arrestee's cell phone may inadvertently access data stored on the "cloud," thus extending "well beyond papers and effects in the physical proximity" of the arrestee).

The magistrate judge suggested that the proposed execution of the Warrant is not extraterritorial because "an SCA Warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data are stored. . . . [I]t places obligations only on the service

---

[27] We thus disagree with the magistrate judge that all of the relevant conduct occurred in the United States. *See In re Warrant*, 15 F. Supp. 3d at 475-76.

[28] The concurring opinion suggests that the privacy interest that is the focus of the statute may not be intrinsically related to the place where the private content is stored, and that an emphasis on place is "suspect when the content consists of emails stored in the 'cloud.'" Concurring Op. at 14 n.7. But even messages stored in the "cloud" have a discernible physical location. Here, we know that the relevant data is stored at a datacenter in Dublin, Ireland. In contrast, it is possible that the identity, citizenship, and location of the user of an online communication account could be unknown to the service provider, the government, and the official issuing the warrant, even when the government can show probable cause that a particular account contains evidence of a crime.

provider to act within the United States." *In re Warrant*, 15 F. Supp. 3d at 475-76. We disagree. First, his narrative affords inadequate weight to the facts that the data is stored in Dublin, that Microsoft will necessarily interact with the Dublin datacenter in order to retrieve the information for the government's benefit, and that the data lies within the jurisdiction of a foreign sovereign. Second, the magistrate judge's observations overlook the SCA's formal recognition of the special role of the service provider vis-à-vis the content that its customers entrust to it. In that respect, Microsoft is unlike the defendant in *Marc Rich* and other subpoena recipients who are asked to turn over records in which only *they* have a protectable privacy interest.

The government voices concerns that, as the magistrate judge found, preventing SCA warrants from reaching data stored abroad would place a "substantial" burden on the government and would "seriously impede[]" law enforcement efforts. *Id.* at 474. The magistrate judge noted the ease with which a wrongdoer can mislead a service provider that has overseas storage facilities into storing content outside the United States. He further noted that the current process for obtaining foreign-stored data is cumbersome. That process is governed by a series of Mutual Legal Assistance Treaties ("MLATs") between the United States and other countries, which allow signatory states to request one another's assistance with ongoing criminal investigations, including issuance and execution of search warrants. *See* U.S. Dep't of State, 7 Foreign Affairs Manual (FAM) § 962.1 (2013), *available at* fam.state.gov/FAM/07FAM/07FAM0960.html (last visited

May 12, 2016) (discussing and listing MLATs).[29] And he observed that, for countries with which it has not signed an MLAT, the United States has no formal tools with which to obtain assistance in conducting law enforcement searches abroad.[30]

These practical considerations cannot, however, overcome the powerful clues in the text of the statute, its other aspects, legislative history, and use of the term of art "warrant," all of which lead us to conclude that an SCA warrant may reach only data stored within United States boundaries. Our conclusion today also serves the interests of comity that, as the MLAT process reflects, ordinarily govern the conduct of cross-boundary criminal investigations. Admittedly, we cannot be certain of the scope of the obligations that

---

[29] The United States has entered into an MLAT with all member states of the European Union, including Ireland. *See* Agreement on Mutual Legal Assistance Between the European Union and the United States of America, June 25, 2003, T.I.A.S. No. 10-201.1.

[30] In addition, with regard to the foreign sovereign's interest, the District Court described § 442(1)(a) of the Restatement of Foreign Relations Law as "dispositive." Tr. of Oral Arg., *supra* note 25, at 69. That section provides:

> A court or agency in the United States, when authorized by statute or rule of court, [is empowered to] order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States.

Restatement of Foreign Relations Law (3d) § 442(1)(a) (1987). We are not persuaded. The predicate for the Restatement's conclusion is that the court ordering production of materials located outside the United States is "authorized by statute or rule of court" to do so. Whether such a statute—the SCA—can fairly be read to authorize the production sought is precisely the question before us.

the laws of a foreign sovereign—and in particular, here, of Ireland or the E.U.—place on a service provider storing digital data or otherwise conducting business within its territory. But we find it difficult to dismiss those interests out of hand on the theory that the foreign sovereign's interests are unaffected when a United States judge issues an order requiring a service provider to "collect" from servers located overseas and "import" into the United States data, possibly belonging to a foreign citizen, simply because the service provider has a base of operations within the United States.

Thus, to enforce the Warrant, insofar as it directs Microsoft to seize the contents of its customer's communications stored in Ireland, constitutes an unlawful extraterritorial application of the Act.

CONCLUSION

We conclude that Congress did not intend the SCA's warrant provisions to apply extraterritorially. The focus of those provisions is protection of a user's privacy interests. Accordingly, the SCA does not authorize a U.S. court to issue and enforce an SCA warrant against a United States-based service provider for the contents of a customer's electronic communications stored on servers located outside the United States. The SCA warrant in this case may not lawfully be used to compel Microsoft to produce to the government the contents of a customer's e-mail account stored exclusively in Ireland. Because Microsoft has otherwise complied with the Warrant, it has no remaining lawful obligation to produce materials to the government.

We therefore **REVERSE** the District Court's denial of Microsoft's motion to quash; we **VACATE** its order holding Microsoft in civil contempt of court; and we **REMAND** this cause to the District Court with instructions to quash the warrant insofar as it demands user content stored outside of the United States.

GERARD E. LYNCH, *Circuit Judge*, concurring in the judgment:

I am in general agreement with the Court's conclusion that, in light of the presumption against extraterritorial application of congressional enactments, the Stored Communications Act ("SCA" or the "Act") should not, on the record made by the government below, be construed to require Microsoft to turn over records of the content of emails stored on servers in Ireland. I write separately to clarify what, in my view, is at stake and not at stake in this case; to explain why I believe that the government's arguments are stronger than the Court's opinion acknowledges; and to emphasize the need for congressional action to revise a badly outdated statute.

I

An undercurrent running through Microsoft's and several of its amici's briefing is the suggestion that this case involves a government threat to individual privacy. I do not believe that that is a fair characterization of the stakes in this dispute. To uphold the warrant here would not undermine basic values of privacy as defined in the Fourth Amendment and in the libertarian traditions of this country.

As the majority correctly points out, the SCA presents a tiered set of requirements for government access to electronic communications and information relating to them. Although Congress adopted the Act in order to provide some privacy protections to such communications, *see* H.R. Rep. No. 99-647, at 21-23 (1986); S. Rep. No. 99-541, at 3 (1986), those requirements are in many ways less protective of privacy than

many might think appropriate. *See, e.g.*, *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) (holding that the SCA violates the Fourth Amendment to the extent that it allows government agents to obtain the contents of emails without a warrant);[1] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1214 (2004) (emphasizing that "[t]he SCA is not a catch-all statute designed to protect the privacy of stored Internet communications" and that "there are many problems of Internet privacy that the SCA does not address"). But this case does not require us to address those arguable defects in the statute. That is because in this case, the government complied with the most restrictive privacy-protecting requirements of the Act. Those requirements are consistent with the highest level of protection ordinarily required by the Fourth Amendment for the issuance of search warrants: a demonstration by the government to an independent judicial officer that evidence presented on oath justifies the conclusion that there is probable cause to believe that a crime has been committed, and that evidence of such crime can be found in the communications sought by the government.

That point bears significant emphasis. In this case, the government proved to the satisfaction of a judge that a reasonable person would believe that the records sought contained evidence of a crime. That is the

---

[1] In the wake of *Warshak*, it has apparently been the policy of the Department of Justice since 2013 always to use warrants to require the disclosure of the contents of emails under the SCA, even when the statute permits lesser process. H.R. Rep. No. 114-528, at 9 (2016).

showing that the framers of our Bill of Rights believed was sufficient to support the issuance of search warrants. U.S. Const. amend. IV ("[N]o Warrants shall issue, but upon probable cause. . . . "). In other words, in the ordinary domestic law enforcement context, if the government had made an equivalent showing that evidence of a crime could be found in a citizen's home, that showing would permit a judge to authorize law enforcement agents to forcibly enter that home and search every area of the home to locate the evidence in question, and even (if documentary or electronic evidence was sought) to rummage through file cabinets and to seize and examine the hard drives of computers or other electronic devices. That is because the Constitution protects "[t]he right of the people to be secure in their persons, houses, papers and effects" not absolutely, but only "against *unreasonable* searches and seizures," *id.* (emphasis added), and strikes the balance between the protection of privacy and the needs of law enforcement by requiring, in most cases, a warrant supported by a judicial finding of probable cause before the most intrusive of searches can take place. *See, e.g.*, *Riley v. California*, 134 S. Ct. 2473, 2482 (2014).

Congress, of course, is free to impose even stricter requirements on specific types of searches—and it has occasionally done so, for example in connection with the real-time interception of communications (as in wiretapping and electronic eavesdropping). *See* 18 U.S.C. § 2518(3)(a) (permitting the approval of wiretap applications only in connection with investigations of certain enumerated crimes); *id.* § 2518(3)(c) (requiring that a judge find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous"

before a wiretap application can be approved). But it has not done so for permitting government access to any category of *stored* electronic communications, and Microsoft does not challenge the constitutional adequacy of the protections provided by the Act to those communications. Put another way, Microsoft does not argue here that, if the emails sought by the government were stored on a server at its headquarters in Redmond, Washington, there would be any constitutional obstacle to the government's acquiring them by the same means that it used in this case. Indeed, as explained above, the showing made by the government would support a warrant that permitted agents to forcibly enter those headquarters and seize the server itself.

I emphasize these points to clarify that Microsoft's argument is not that the government does not have sufficiently solid information, and sufficiently important interests, to justify invading the privacy of the customer whose emails are sought and acquiring records of the contents of those emails. Microsoft does not ask the Court to create, as a matter of constitutional law, stricter safeguards on the protection of those emails—and the Court does not do so. Rather, the sole issue involved is whether Microsoft can thwart the government's otherwise justified demand for the emails at issue by the simple expedient of choosing—in its own discretion—to store them on a server in another country.

That discretion raises another point about privacy. Under Microsoft's and the Court's interpretation of the SCA, the privacy of Microsoft's customers' emails is dependent not on the traditional constitutional safe-

guard of private communications—judicial oversight of the government's conduct of criminal investigations—but rather on the business decisions of a private corporation. The contract between Microsoft and its customers does not limit the company's freedom to store its customers' emails wherever it chooses, and if Microsoft chooses, for whatever reasons of profit or cost control, to repatriate the emails at issue here to a server in United States, there will be no obstacle to the government's obtaining them. As the Court points out, Microsoft does in fact choose to locate the records of anyone who *says* that he or she resides in the United States on domestic servers. It is only *foreign* customers, and those Americans who *say* that they reside abroad, who gain any enhanced protection from the Court's holding. And that protection is not merely enhanced, it is *absolute*: the government can never obtain a warrant that would require Microsoft to turn over those emails, however certain it may be that they contain evidence of criminal activity, and even if that criminal activity is a terrorist plot.[2] Or to be more precise, the customer's privacy in that case is absolute *as against the government*; her privacy is protected

---

[2] Although the Court does not reach the question, its opinion strongly suggests that that protection is absolute in the further sense that it applies also to less-protected categories of information otherwise reachable by the SCA's other disclosure-compelling instruments—subpoenas and court orders. If, as the Court holds, the "focus" of the SCA is privacy, and the relevant territorial locus of the privacy interest is where the customer's protected content is stored, *see* Majority Op. at 39, the use of the SCA to compel the disclosure of *any* email-related records stored abroad is impermissibly extraterritorial, regardless of the category of information or disclosure order.

against *Microsoft* only to the extent defined by the terms of her (adhesion) contract with the company.

Reasonable people might conclude that extremely stringent safeguards ought to apply to government investigators' acquisition of the contents of private email communications, and that the provisions of the SCA, as applied domestically, should be enhanced to provide even greater privacy, at an even higher cost to criminal investigations. Other reasonable people might conclude that, at least in some cases, investigators should have freer access to stored communications. It is the traditional task of Congress, in enacting legislation, and of the courts, in interpreting the Fourth Amendment, to strike a balance between privacy interests and law enforcement needs. But neither privacy interests nor the needs of law enforcement vary depending on whether a private company chooses to store records here or abroad—particularly when the "records" are electronic zeros and ones that can be moved around the world in seconds, and *will* be so moved whenever it suits the convenience or commercial purposes of the company. The issue facing the Court, then, is not actually about the need to enhance privacy protections for information that Americans choose to store in the "cloud."

II

In emphasizing the foregoing, I do not for a moment mean to suggest that this case is not important, or that significant non-privacy interests may not justify a congressional decision to distinguish records stored domestically from those stored abroad. It is important to recognize, however, that the dispute here is not about privacy, but rather about the international reach

of American law. That question is important in its own right, and some further clarifications are in order about the division of responsibility between the courts and Congress in addressing it.

The courts have a significant role in the protection of privacy, because the Constitution sets limits on what even the elected representatives of the people can authorize when it comes to searches and seizures. Specifically, the courts have an independent responsibility to interpret the Fourth Amendment, an explicit check on Congress's power to authorize unreasonable searches. What searches are unreasonable is of course a difficult question, particularly when courts are assessing statutory authorizations of novel types of searches to deal with novel types of threat. In that context, courts need to be especially cautious, and respectful of the judgments of Congress. *See, e.g., ACLU v. Clapper*, 785 F.3d 787, 824-25 (2d Cir. 2015). But it is ultimately the courts' responsibility to ensure that constitutional restraints on searches and seizures are respected.

Whether American law applies to conduct occurring abroad is a different type of question. That too is sometimes a difficult question. It will often be tempting to attempt to protect American interests by extending the reach of American law and undertaking to regulate conduct that occurs beyond our borders. But there are significant practical and policy limitations on the desirability of doing so. We live in a system of independent sovereign nations, in which other countries have their own ideas, sometimes at odds with ours, and their own legitimate interests. The attempt to apply U.S. law to conduct occurring abroad can cause ten-

sions with those other countries, most easily appreciated if we consider the likely American reaction if France or Ireland or Saudi Arabia or Russia proclaimed its right to regulate conduct by Americans within our borders.

But the decision about whether and when to apply U.S. law to actions occurring abroad is a question that is left entirely to Congress. *See Benz v. Compania Naviera Hidalgo, S.A.*, 353 U.S. 138, 147 (1957) (Congress "alone has the facilities necessary to make fairly [the] important policy decision" whether a statute applies extraterritorially). No provision of the Constitution limits Congress's power to apply its laws to Americans, or to foreigners, abroad, and Congress has on occasion done so, expressly or by clear implication. The courts' job is simply to do their best to understand what Congress intended. Where Congress has clearly indicated that a law applies extraterritorially, as for example in 18 U.S.C. § 2332(a), which prohibits the murder of U.S. citizens abroad, the courts apply the law as written. *See RJR Nabisco, Inc. v. European Cmty.*, 579 U.S. __, __, 2016 WL 3369423, at *9-10 (June 20, 2016). We do the same when a law clearly applies only domestically.

The latter situation is far more common, so common that it is the ordinary presumption. When Congress makes it a crime to "possess a controlled substance," 21 U.S.C. § 844(a), it does not say that it is a crime to possess dangerous or addictive drugs *in the United States*. It speaks absolutely, as if proclaiming a universal rule, but we understand that the law applies only here; it does not prohibit the possession of marijuana by a Dutchman, or even by an American, in the Nether-

lands. "Congress generally legislates with domestic concerns in mind," *RJR Nabisco*, 2016 WL 3369423, at *8, quoting *Smith v. United States*, 507 U.S. 197, 204 n.5 (1993), and so, unless Congress clearly indicates to the contrary, we presume that statutes have only domestic effect.

I have little trouble agreeing with my colleagues that the SCA does not have extraterritorial effect. As the Supreme Court recently made clear in *RJR Nabisco*, the presumption applies not only to statutes that straightforwardly regulate or criminalize conduct, but also to jurisdictional, procedural and remedial statutes. *Id.* at *15-16; *see also Loginovskaya v. Batratchenko*, 764 F.3d 266, 272 (2d Cir. 2014) (rejecting the argument that the presumption "governs substantive (conduct-regulating) provisions rather than procedural provisions"). Moreover, *RJR Nabisco* also reemphasized that the relevant question is not whether we think Congress "would have wanted" the statute to apply extraterritorially had it foreseen the precise situation before us, but whether it made clear its intention to give the statute extraterritorial effect. *RJR Nabisco*, 2016 WL 3369423, at *7. There is no indication whatsoever in the text or legislative history that Congress intended the Act to have application beyond our borders. It would be quite surprising if it had. The statute was adopted in the early days of what is now the internet, when Congress could hardly have foreseen that multinational companies providing digital services of all sorts would one day store vast volumes of communications and other materials for ordinary people and easily be able to move those materials across borders at lightning speed. *See* Majority Op. at 14.

The tricky part, in a world of transnational transactions taking place in multiple jurisdictions at once, is deciding whether a proposed application of a statute is domestic or extraterritorial. That determination can be complicated even for criminal acts when they touch on multiple jurisdictions, but the problem is particularly acute when we deal not with a simple effort to regulate behavior that—given the physical limitations of human bodies—can often be fixed to a specific location, but with statutes that operate in more complex fashions. If SCA warrants were traditional search warrants, permitting law enforcement agents to search a premises and seize physical objects, the extraterritoriality question would be relatively easy: a warrant authorizing a search of a building physically located in Ireland would plainly be an extraterritorial application of the statute (and it would be virtually inconceivable under ordinary notions of international law that Congress would ever attempt to authorize any such thing). But as the government points out, this case differs from that classic scenario with respect to both the nature of the legal instrument involved and the nature of the evidentiary material the government seeks.

First, the "warrant" required for the government to obtain the emails sought in this case does not appear to be a traditional search warrant. Significantly, the SCA does not describe the warrant as a *search* warrant. Nor does it contain language implying (let alone saying outright) that the warrant to which it refers authorizes government agents to go to the premises of a service provider without prior notice to the provider, search those premises until they find the computer, server or other device on which the sought communications reside, and seize that device (or duplicate and "seize" the rel-

evant data it contains).[3] Rather, the statute expressly requires the "warrant" not to authorize a search or seizure, but as the procedural mechanism to allow the government to "require a [service provider] to disclose the contents of [certain] electronic communication[s]" *without notice to the subscriber or customer.* 18 U.S.C. § 2703(b)(1)(A). Parallel provisions permit the government to require equivalent disclosure of the communications by the service provider by a simple administrative subpoena or by a court order, provided only that notice is provided to the subscriber. *Id.* § 2703(b)(1)(B).[4] Indeed, the various methods of obtain-

---

[3] I do note, however, that the particular warrant in this case states that the government "requests the search of" a "PREMISES" and "COMMAND[S]" an officer to "execute" the warrant on or before a certain date and time. J.A. 44. Neither party argues that this case turns on the language in the warrant itself, and the government explains that this language was included only because the warrant "was prepared using the generic template for search warrants." Gov't Br. 20. Nevertheless, it is worth emphasizing that the government itself chose the "template" it used to create the warrant it then asked the magistrate judge to sign. It is, to say the least, unimaginative for the government to utilize a warrant form that purports to authorize conduct that the statute under which it is obtained plainly does not permit, and then to turn around and argue that this sort of warrant is completely different from what its language tells us it is, and that the language is unimportant because the government simply used the same formal template it uses under other, more traditional circumstances involving physical searches.

[4] One category of communications—those held "in electronic storage" by an electronic communication service for one hundred and eighty days or less—is reachable only by SCA warrant, with or without notice to the customer. 18 U.S.C. § 2703(a). But, although we ourselves have not addressed the issue, the majority view is that, once the user of an entirely web-based email service (such as

ing the communications, with or without notice, are not merely parallel—they all depend on the same verbal phrase. They are simply alternative means, applicable in different circumstances, to "require [the service provider] to disclose [the communications]." *Id.* § 2703(a), (b).

This difference is significant if we are looking to determine the "focus" of the SCA for purposes of determining whether a particular application of the statute is or is not extraterritorial. *See Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247, 266-69 (2010). A search warrant "particularly describing the place to be searched, and the persons or things to be seized," U.S. Const. amend. IV, is naturally seen as focused on the *place* to be searched; as explained above, if the government argued that a statute authorized a search of a place outside the United States, that would clearly be an extraterritorial application of the statute. Here,

---

Microsoft's) opens an email he has received, that email is no longer "in electronic storage" on an electronic communication service. *See Lazette v. Kulmatycki*, 949 F. Supp. 2d 748, 758 (N.D. Ohio 2013); *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010); *United States v. Weaver*, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009); *Jennings v. Jennings*, 736 S.E.2d 242, 245 (S.C. 2012); *id.* at 248 (Toal, C.J., concurring in the result); Kerr, *A User's Guide*, *supra*, at 1216-18 & n.61; *cf. Anzaldua v. Ne. Ambulance & Fire Prot. Dist.*, 793 F.3d 822, 840-42 (8th Cir. 2015) (message retained on Gmail server in "sent" folder was not in electronic storage). *But see Cheng v. Romo*, Civ. No. 11-10007-DJC, 2013 WL 6814691, at *3-5 (D. Mass. Dec. 20, 2013); *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008); *cf. Theofel v. Farey-Jones*, 359 F.3d 1066, 1075-77 (9th Cir. 2003) (message is in electronic storage until it "has expired in the normal course"). Under that reading of the statute, only emails that have not yet been opened by the recipient fall into the category described above.

however, the SCA warrant provision does not purport to authorize any such thing. Just like the parallel subpoena and court order provisions, it simply authorizes the government to *require the service provider to disclose* certain communications to which it has access.[5]

---

[5] Although the Supreme Court has not addressed the question, there is considerable case law, including in this circuit, permitting the exercise of subpoena powers in precisely the situation in which the government demands records located abroad from an American company, or a foreign company doing business here. *See, e.g.*, *Linde v. Arab Bank, PLC*, 706 F.3d 92 (2d Cir. 2013); *United States v. Bank of Nova Scotia*, 740 F.2d 817 (11th Cir. 1984); *Marc Rich & Co., A.G. v. United States*, 707 F.2d 663 (2d Cir. 1983); *United States v. First Nat'l City Bank*, 396 F.2d 897, 900-01 (2d Cir. 1968) ("It is no longer open to doubt that a federal court has the power to require the production of documents located in foreign countries if the court has in personam jurisdiction of the person in possession or control of the material."). At least as far as American courts are concerned (some foreign governments may think otherwise), such demands for the production of records are not seen as categorically impermissible extraterritorial uses of American investigatory powers, in the way that search warrants for foreign locations certainly would be. *Compare* Restatement (Third) of Foreign Relations Law § 442(1)(a) ("A court or agency in the United States, when authorized by statute or rule of court, may order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States.") *with id.* § 433(1) ("Law enforcement officers of the United States may exercise their functions in the territory of another state only (a) with the consent of the other state and if duly authorized by the United States; and (b) in compliance with the laws both of the United States and of the other state.").

Microsoft attempts to distinguish the cases cited above on the ground that the subpoenas in those cases required their recipients to disclose only the contents of their own business records, and not the records of a third party "held in trust" by the recipients. Appellant's Br. 48. "Email correspondance," Microsoft explains,

The government quite reasonably argues that the focus of such a provision is not on the place where the service provider stores the communications, but on the place where the service provider discloses the information to the government, as requested.[6]

---

is unlike bank records because it "is personal, even intimate," and "can contain the sum of an individual's private life." *Id.* at 44 (internal quotation marks omitted). Even assuming, however, that Microsoft accurately characterizes the cases it seeks to distinguish, *but cf. In re Horowitz*, 482 F.2d 72 (2d Cir. 1973) (partially upholding a subpoena requiring an accountant to produce the contents of three locked file cabinets belonging to a client), this privacy-based argument is, as explained above, a red herring. Microsoft does not dispute that the government could have required the disclosure of the emails at issue here if they were stored in the United States, and Microsoft's decision to store them abroad does not obviously entitle their owner to any higher degree of privacy protection.

[6] As the government notes, the selection of the term "warrant" to describe an instrument that does not operate like a traditional arrest or search warrant is easily explained by the fact that the provision in question, which permits government access to a person's stored communications without notice to that person, provides the highest level of privacy protection in the statute: the requirement that an independent judicial officer determine that probable cause exists to believe that a crime has been committed and that evidence of that crime may be found in the communications demanded. The *showing* necessary to obtain judicial authorization to require the service provider to disclose the communications is that associated with traditional warrants; the *manner* in which the disclosure is obtained by the government, however, is more closely analogous to the workings of subpoenas and court-ordered discovery: the government serves the service provider with an order from a court that requires the *service provider* to look within its records and *disclose* the specified information to the government; it does not present to the service provider a court order that permits *government agents* to search

The nature of the records demanded is also relevantly different from that of the physical documents sought by traditional search warrants. Tangible documents, having a material existence in the physical world, are stored in a particular physical location. Executing a traditional search warrant requires a visit to that location, to visually inspect the documents to select the responsive materials and to take those materials away. Even when tangible documents are sought by subpoena, rather than by search warrant, it is arguable that the focus of the subpoena, for extraterritoriality purposes, is on the place where the documents are stored, since in order to comply with a subpoena seeking documents stored abroad, corporate employees will have to be present in the foreign location where the documents exist to inspect and select the relevant documents, which will then have to be transported out of that location and into the United States.

Electronic "documents," however, are different. Their location on a computer server in a foreign country is, in important ways, merely virtual. *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 408 (2014) (explaining that "the very idea of online data being located in a particular physical 'place' is becoming rapidly outdated," because computer files can be fragmented and dispersed across many servers). Corporate employees in the United States can review those records, when responding to the "warrant" or subpoena or court order just as they can do in the ordinary course of business, and provide the relevant materials to the demanding government

---

through the service provider's premises and documents and *seize* the specified information.

agency, without ever leaving their desks in the United States. The entire process of compliance takes place domestically.

The government's characterization of the warrant at issue as domestic, rather than extraterritorial, is thus far from frivolous, and renders this, for me, a very close case to the extent that the presumption against extraterritoriality shapes our interpretation of the statute. One additional potential fact heightens the complexity. We do not know, on this record, whether the customer whose emails were sought by the government is or is not a United States citizen or resident. It is not clear that whether the customer is a United States person or not matters to the rather simplistic "focus" test adopted by the Supreme Court in *Morrison*, although it would have mattered to the more flexible test utilized by the Second Circuit in that case. *See Morrison v. Nat'l Australia Bank Ltd.*, 547 F.3d 167, 171 (2d Cir. 2008). But it seems to me that it *should* matter. The Supreme Court has rightly pointed out that the presumption against extraterritoriality is more than simply a means for avoiding conflict with foreign laws. *See Morrison*, 561 U.S. at 255. At the same time, the presumption that Congress legislates with domestic concerns pre-eminent in its collective mind does not fully answer the question what those domestic concerns are in any given case. *See id.* at 266. Particularly in connection with statutes that provide tools to law enforcement, one imagines that Congress is concerned with balancing liberty interests of various kinds against the need to enforce *domestic* law. Thus, when Congress authorizes the (American) government to obtain access to certain information, one might imagine that its focus is on balancing the liberty interests of

Americans (and of other persons residing in the U.S.) against the need to enforce *American* laws. Congress might also reasonably be concerned about the diplomatic consequences of over-extending the reach of American law enforcement officials. This suggests a more complex balancing exercise than identifying a single "focus" of the legislation, the latter approach being better suited to determining whether given *conduct* fitting within the literal words of a prohibition should be characterized as domestic or extraterritorial.[7]

Because Microsoft relies solely on customers' self-reporting in classifying customers by residence, and stores emails (but only for the most part, and only in the interests of efficiency and good customer service) on local servers—and because the government did not include in its warrant application such information, if any, as it had about the target of its investigation—we

---

[7] While, for these reasons, it may be impossible to answer satisfactorily the question what the single focus of the SCA is, I note that I have considerable doubts about the answer supplied by the Court, which holds that the SCA provisions at issue here "focus on protecting the privacy of the content of a user's stored electronic communications." Majority Op. at 33. Privacy, however, is an abstract concept with no obvious territorial locus; the conclusion that the SCA's focus is privacy thus does not really help us to distinguish domestic applications of the statute from extraterritorial ones. "The real motor of the Court's opinion," *Morrison*, 561 U.S. at 284 (Stevens, *J.*, concurring in the judgment), then, is less the conclusion that the statute focuses on privacy than the majority's further determination that the locus of the invasion of privacy is where the private content is stored—a determination that seems to me suspect when the content consists of emails stored in the "cloud." It seems at least equally persuasive that the invasion of privacy occurs where the person whose privacy is invaded customarily resides.

do not know the nationality of the customer. If he or she is Irish (as for all we know the customer is), the case might present a troubling prospect from an international perspective: the Irish government and the European Union would have a considerable grievance if the United States sought to obtain the emails of an Irish national, stored in Ireland, from an American company which had marketed its services to Irish customers in Ireland. The case looks rather different, however—at least to me, and I would hope to the people and officials of Ireland and the E.U.—if the American government is demanding from an American company emails of an American citizen resident in the U.S., which are accessible at the push of a button in Redmond, Washington, and which are stored on a server in Ireland only as a result of the American customer's misrepresenting his or her residence, for the purpose of facilitating domestic violations of American law, by exploiting a policy of the American company that exists solely for reasons of convenience and that could be changed, either in general or as applied to the particular customer, at the whim of the American company. Given that the extraterritoriality inquiry is essentially an effort to capture the congressional will, it seems to me that it would be remarkably formalistic to classify such a demand as an extraterritorial application of what is effectively the subpoena power of an American court.

These considerations give me considerable pause about treating SCA warrants as extraterritorial whenever the service provider from whom the government seeks to require production has chosen to store the communications on a server located outside the United States. Despite that hesitation, however, I conclude

that my colleagues have ultimately reached the correct result. If we frame the question as whether Congress has demonstrated a clear intention to reach situations of this kind in enacting the Act, I think the better answer is that it has not, especially in the case (which could well be this one) of records stored at the behest of a foreign national on servers in his own country. The use of the word "warrant" may not compel the conclusion that Congress intended to reach only domestically-stored communications that could be reached by a conventional search warrant, because, for the reasons given above, that label should not be controlling. *Cf. Big Ridge, Inc. v. Fed. Mine Safety & Health Review Comm'n*, 715 F.3d 631, 645-46 (7th Cir. 2013) (explaining that "we look to the substance of [the government's] inspection power rather than how the Act nominally refers to those powers," and holding that document requests under the Mine Safety and Health Act of 1977 should be treated as administrative subpoenas rather than as a search or seizure). But it is hard to believe that Congress would have used such a loaded term, and incorporated by reference the procedures applicable to purely domestic warrants, if it had given any thought at all to potential transnational applications of the statute. Nor is it likely that Congress contemplated such applications for a single moment. The now-familiar idea of "cloud" storage of personal electronic data by multinational companies was hardly foreseeable to Congress in 1986, and the related prospects for diplomatic strife and implications for American businesses operating on an international scale were surely not on the congressional radar screen when the Act was adopted. We should not lightly assume that Congress chose to permit SCA warrants

for communications stored abroad when there is no sign that it considered the consequences of doing so. *See Kiobel v. Royal Dutch Petroleum Co.*, 133 S. Ct. 1659, 1664 (2013) ("The presumption against extraterritorial application helps ensure that the Judiciary does not erroneously adopt an interpretation of U.S. law that carries foreign policy consequences not clearly intended by the political branches."). Thus, while I think the case is closer—and the government's arguments more potent—than is reflected in the Court's opinion, I come out in the same place.

III

Despite ultimately agreeing with the result in this case, I dwell on the reasons for thinking it close because the policy concerns raised by the government are significant, and require the attention of Congress. I do not urge that Congress write the government's interpretation into the Act. That is a policy judgment on which my own views have no particular persuasive force. My point is simply that the main reason that both the majority and I decide this case against the government is that there is no evidence that Congress has *ever* weighed the costs and benefits of authorizing court orders of the sort at issue in this case. The SCA became law at a time when there was no reason to do so. But there is reason now, and it is up to Congress to decide whether the benefits of permitting subpoena-like orders of the kind issued here outweigh the costs of doing so.

Moreover, while I do not pretend to the expertise necessary to advocate a particular answer to that question, it does seem to me likely that a sensible answer will be more nuanced than the position advanced by

either party to this case. As indicated above, I am skeptical of the conclusion that the mere location abroad of the server on which the service provider has chosen to store communications should be controlling, putting those communications beyond the reach of a purely "domestic" statute. That may be the default position to which a court must revert in the absence of guidance from Congress, but it is not likely to constitute the ideal balance of conflicting policy goals. Nor is it likely that the ideal balance would allow the government free rein to demand communications, wherever located, from any service provider, of whatever nationality, relating to any customer, whatever his or her citizenship or residence, whenever it can establish probable cause to believe that those communications contain evidence of a violation of American criminal law, of whatever degree of seriousness. Courts interpreting statutes that manifestly do not address these issues cannot easily create nuanced rules: the statute either applies extraterritorially or it does not; the particular demand made by the government either should or should not be characterized as extraterritorial. Our decision today is thus ultimately the application of a default rule of statutory interpretation to a statute that does not provide an explicit answer to the question before us. It does not purport to decide what the answer should be, let alone to impose constitutional limitations on the range of solutions Congress could consider.

Congress need not make an all-or-nothing choice. It is free to decide, for example, to set different rules for access to communications stored abroad depending on the nationality of the subscriber or of the corporate service provider. It could provide for access to such

information only on a more demanding showing than probable cause, or only (as with wiretapping) where other means of investigation are inadequate, or only in connection with investigations into extremely serious crimes rather than in every law enforcement context. Or it could adopt other, more creative solutions that go beyond the possibilities evident to federal judges limited by their own experience and by the information provided by litigants in a particular case.

In addition, Congress need not limit itself to addressing the particular question raised by this case. The SCA was adopted in 1986, at a time when the kinds of services provided by "remote computing services" were not remotely as extensive and complex as those provided today, and when the economic and security concerns presented by such services were not remotely as important as they are now. More than a dozen years ago, a leading commentator was expressing the need to reform the Act. *See* Kerr, *A User's Guide*, *supra*, at 1233-42. It would seem to make sense to revisit, among other aspects of the statute, whether various distinctions, such as those between communications stored within the last 180 days and those that have been held longer, between electronic communication services and remote computing services, or between disclosures sought with or without notice to the customer, should be given the degree of significance that the Act accords them in determining the level of privacy protection it provides, or whether other factors should play some role in that determination.[8]

---

[8] As the Court notes, Majority Op. at 28 n.23, the House of Representatives recently passed a bill amending the SCA's required disclosure provisions. Email Privacy Act, H.R. 699, 114th Cong. § 3

Congress has, in the past, proven adept at adopting rules for adapting the basic requirements of the Fourth Amendment to new technologies. The wiretapping provisions of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510-22, for example, proved to be a remarkably stable and effective structure for dealing with the privacy and law enforcement issues raised by electronic surveillance in the telephone era. More recently, Congress was able to address the concerns presented by the mass acquisition of metadata by the National Security Agency by creating a more nuanced statute than that which the NSA had claimed as authority for its actions. *See ACLU v. Clapper*, 804 F.3d 617, 620 (2d Cir. 2015), discussing the USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015). I fully expect that the Justice Department will respond to this decision by seeking legislation to overrule it. If it does so, Congress would do well to take the occasion to address thoughtfully and dispassionately the suitability of many of the statute's provisions to serving contemporary needs. Although I believe that we have reached the correct result as a matter of interpreting the statute before us, I believe even more strongly that the statute

---

(2016). That bill would require the government to obtain a warrant before it can compel the disclosure of the contents of any electronic communication "stored, held, or maintained" by either an electronic communication service or (under certain circumstances) a remote computing service, no matter the length of the period of storage. *Id.* It does not, however, address those provisions' extraterritorial reach or significantly modernize the statute's structure. *See* Kerr, *The Next Generation*, *supra*, at 386-89 (criticizing a proposal similar to the Email Privacy Act for "work[ing] within [the SCA's] outdated framework"). As of this writing, the Senate has not taken any action on the bill.

should be revised, with a view to maintaining and strengthening the Act's privacy protections, rationalizing and modernizing the provisions permitting law enforcement access to stored electronic communications and other data where compelling interests warrant it, and clarifying the international reach of those provisions after carefully balancing the needs of law enforcement (particularly in investigations addressing the most serious kinds of transnational crime) against the interests of other sovereign nations.

* * *

For these reasons, I concur in the result, but without any illusion that the result should even be regarded as a rational policy outcome, let alone celebrated as a milestone in protecting privacy.

APPENDIX B

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

No. 13 Mag. 2814

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

[Filed: Apr. 25, 2014]

MEMORANDUM AND ORDER

JAMES C. FRANCIS IV

United States Magistrate Judge

"The rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactorily, by any current territorially based sovereign." David R. Johnson & David Post, Law and Borders—The Rise of Law in Cyberspace, 48 Stan. L. Rev. 1367, 1375 (1996). In this case I must consider the circumstances under which law enforcement agents in the United States may obtain digital information from abroad. Microsoft Corporation ("Microsoft") moves to quash a search warrant to the extent that it directs Microsoft to produce the contents of one of its customer's e-mails where that information is stored on a server located in Dublin, Ireland. Micro-

soft contends that courts in the United States are not authorized to issue warrants for extraterritorial search and seizure, and that this is such a warrant. For the reasons that follow, Microsoft's motion is denied.

Background

Microsoft has long owned and operated a web-based e-mail service that has existed at various times under different internet domain names, including Hotmail.com, MSN.com, and Outlook.com. (Declaration of A.B. dated Dec. 17, 2013 ("A.B. Decl."), ¶ 3).[1] Users of a Microsoft e-mail account can, with a user name and a password, send and receive email messages as well as store messages in personalized folders. (A.B. Decl., ¶ 3). E-mail message data include both content information (the message and subject line) and non-content information (such as the sender address, the recipient address, and the date and time of transmission). (A.B. Decl., ¶ 4).

Microsoft stores e-mail messages sent and received by its users in its datacenters. Those datacenters exist at various locations both in the United States and abroad, and where a particular user's information is stored depends in part on a phenomenon known as "network latency"; because the quality of service decreases the farther a user is from the datacenter where his account is hosted, efforts are made to assign each account to the closest datacenter. (A.B. Decl., ¶ 6). Accordingly, based on the "country code" that the customer enters at registration, Microsoft may migrate

---

[1] Pursuant to an application by Microsoft, certain information that is commercially sensitive, including the identity of persons who submitted declaration, has been redacted from public filings.

the account to the datacenter in Dublin. (A.B. Decl., ¶ 7). When this is done, all content and most non-content information associated with the account is deleted from servers in the United States. (A.B. Decl., ¶ 7).

The non-content information that remains in the United States when an account is migrated abroad falls into three categories. First, certain non-content information is retained in a data warehouse in the United States for testing and quality control purposes. (A.B. Decl., ¶ 10). Second, Microsoft retains "address book" information relating to certain web-based e-mail accounts in an "address book clearing house." (A.B. Decl., ¶ 10). Finally, certain basic non-content information about all accounts, such as the user's name and country, is maintained in a database in the United States. (A.B. Decl., ¶ 10).

On December 4, 2013, in response to an application by the United States, I issued the search warrant that is the subject of the instant motion. That warrant authorizes the search and seizure of information associated with a specified web-based e-mail account that is "stored at premises owned, maintained, controlled, or operated by Microsoft Corporation, a company headquartered at One Microsoft Way, Redmond, WA." (Search and Seizure Warrant ("Warrant"), attached as Exh. 1 to Declaration of C.D. dated Dec. 17, 2013 ("C.D. Decl."), Attachment A). The information to be disclosed by Microsoft pursuant to the warrant consists of:

a. The contents of all e-mails stored in the account, including copies of e-mails sent from the account;

b. All records or other information regarding the identification of the account, to include full name,

> physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and sources of payment (including any credit or bank account number);
>
> c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;
>
> d. All records pertaining to communications between MSN . . . and any person regarding the account, including contacts with support services and records of actions taken.

(Warrant, Attachment C, ¶ I(a)-(d)).

It is the responsibility of Microsoft's Global Criminal Compliance ("GCC") team to respond to a search warrant seeking stored electronic information. (C.D. Decl., ¶ 3). Working from offices in California and Washington, the GCC team uses a database program or "tool" to collect the data. (C.D. Decl., ¶¶ 3, 4). Initially, a GCC team member uses the tool to determine where the data for the target account is stored and then collects the information remotely from the server where the data is located, whether in the United States or elsewhere. (C.D. Decl., ¶¶ 5, 6).

In this case, Microsoft complied with the search warrant to the extent of producing the non-content information stored on servers in the United States.

However, after it determined that the target account was hosted in Dublin and the content information stored there, it filed the instant motion seeking to quash the warrant to the extent that it directs the production of information stored abroad.

Statutory Framework

The obligation of an Internet Service Provider ("ISP") like Microsoft to disclose to the Government customer information or records is governed by the Stored Communications Act (the "SCA"), passed as part of the Electronic Communications Privacy Act of 1986 (the "ECPA") and codified at 18 U.S.C. §§ 2701-2712. That statute authorizes the Government to seek information by way of subpoena, court order, or warrant. The instrument law enforcement agents utilize dictates both the showing that must be made to obtain it and the type of records that must be disclosed in response.

First, the Government may proceed upon an "administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena." 18 U.S.C. § 2703(b)(1)(B)(i). In response, the service provider must produce (1) basic customer information, such as the customer's name, address, Internet Protocol connection records, and means of payment for the account, 18 U.S.C. § 2703(c)(2); unopened e-mails that are more than 180 days old, 18 U.S.C. § 2703(a); and any opened e-mails, regardless of age, 18 U.S.C.

§§ 2703(b)(1)(B)(i).[2] The usual standards for issuance of compulsory process apply, and the SCA does not

---

[2] The distinction between opened and unopened e-mail does not appear in the statute. Rather, it is the result of interpretation of the term "electronic storage," which affects whether the content of an electronic communication is subject to rules for a provider of electronic communications service ("ECS"), 18 U.S.C. § 2703(a), or those for a provider of remote computing service ("RCS"), 18 U.S.C. § 2703(b). The SCA regulates the circumstances under which "[a] governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication [] that is in electronic storage in an electronic communications system. . . . " 18 U.S.C. § 2703(a). "Electronic storage" is in turn defined as "(A) any temporary intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for the purposes of backup protection of such communication." 18 U.S.C. § 2510(17). While most courts have held that an e-mail is no longer in electronic storage once it has been opened by the recipient, see, e.g., Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 987 (C.D. Cal. 2010); United States v. Weaver, 636 F. Supp. 2d 769, 771-73 (C.D. Ill. 2009); see also Owen S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208, 1216 (2004) (hereinafter A User's Guide) ("The traditional understanding has been that a copy of an opened e-mail sitting on a server is protected by the RCS rules, not the ECS rules"), the Ninth Circuit has instead focused on whether "the underlying message has expired in the normal course," Theofel v. Farley-Jones, 359 F.3d 1066, 1076 (9th Cir. 2004); see also id. at 1077 ("[W]e think that prior access is irrelevant to whether the messages at issue were in electronic storage."). Resolution of this debate is unnecessary for purposes of the issue before me.

Likewise, it is not necessary to determine whether Microsoft was providing ECS or RCS in relation to the communications in question. The statute defines ECS as "any service which provides users thereof the ability to send or receive wire or electronic com-

impose any additional requirements of probable cause or reasonable suspicion. However, the Government may obtain by subpoena the content of e-mail only if prior notice is given to the customer. 18 U.S.C. § 2703(b)(1)(B)(i).

If the Government secures a court order pursuant to 18 U.S.C. § 2703(d), it is entitled to all of the information subject to production under a subpoena and also "record[s] or other information pertaining to a subscriber [] or customer," such as historical logs showing the e-mail addresses with which the customer had communicated. 18 U.S.C. § 2703(c)(1). In order to obtain such an order, the Government must provide the court with "specific and articulable facts showing that there are reasonable grounds to believe that the content of a wire or electronic communication, or the rec-

---

munications," 18 U.S.C. § 2510(15), while RCS provides "to the public [] computer storage or processing services by means of an electronic communications system, 18 U.S.C. § 2711(2). Since service providers now generally perform both functions, the distinction, which originated in the context of earlier technology, is difficult to apply. See Crispin, 717 F. Supp. 2d at 986 n.42; In re Application of the United States of America for a Search Warrant for Contents of Electronic Mail and for an Order Directing a Provider of Electronic Communication Services to not Disclose the Existence of the Search Warrant, 665 F. Supp. 2d 1210, 1214 (D. Or. 2009) (hereinafter In re United States) ("Today, most ISPs provide both ECS and RCS; thus, the distinction serves to define the service that is being provided at a particular time (or as to a particular piece of electronic communication at a particular time), rather than to define the service provider itself."); Kerr, A User's Guide at 1215 ("The distinction of providers of ECS and RCS is made somewhat confusing by the fact that most network service providers are multifunctional. They can act as providers of ECS in some contexts, providers of RCS in some contexts, and as neither in some contexts as well.").

ords or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. 2703(d).

Finally, if the Government obtains a warrant under section 2703(a) (an "SCA Warrant"), it can compel a service provider to disclose everything that would be produced in response to a section 2703(d) order or a subpoena as well as unopened e-mails stored by the provider for less than 180 days. In order to obtain an SCA Warrant, the Government must "us[e] the procedures described in the Federal Rules of Criminal Procedure" and demonstrate probable cause. 18 U.S.C. § 2703(a); see Fed. R. Crim. P. 41(d)(1) (requiring probable cause for warrants).

Discussion

Microsoft's argument is simple, perhaps deceptively so. It notes that, consistent with the SCA and Rule 41 of the Federal Rules of Criminal Procedure, the Government sought information here by means of a warrant. Federal courts are without authority to issue warrants for the search and seizure of property outside the territorial limits of the United States. Therefore, Microsoft concludes, to the extent that the warrant here requires acquisition of information from Dublin, it is unauthorized and must be quashed.

That analysis, while not inconsistent with the statutory language, is undermined by the structure of the SCA, by its legislative history, and by the practical consequences that would flow from adopting it.

A. Statutory Language

In construing federal law, the "starting point in discerning congressional intent is the existing statutory language." Lamie v. United States Trustee, 540 U.S. 526, 534 (2004) (citing Hughes Aircraft Co. v. Jacobson, 525 U.S. 432, 438 (1999). "And where the statutory language provides a clear answer, [the analysis] ends there as well." Hughes Aircraft Co., 525 U.S. at 438. However, a court must search beneath the surface of text that is ambiguous, that is, language that is "capable of being understood in two or more possible senses or ways." Chickasaw Nation v. United States, 534 U.S. 84, 90 (1985) (internal quotation marks omitted).

Here, the relevant section of the SCA provides in pertinent part:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction.

18 U.S.C. § 2703(a). This language is ambiguous in at least one critical respect. The words "using the procedures described in the Federal Rules of Criminal Procedure" could be construed to mean, as Microsoft argues, that all aspects of Rule 41 are incorporated by reference in section 2703(a), including limitations on the territorial reach of a warrant issued under that rule. But, equally plausibly, the statutory language

could be read to mean that while procedural aspects of the application process are to be drawn from Rule 41 (for example, the presentation of the application based on sworn testimony to a magistrate judge), more substantive rules are derived from other sources. See In re United States, 665 F. Supp. 2d at 1219 (finding ambiguity in that "'[i]ssued' may be read to limit the procedures that are applicable under § 2703(a), or it might merely have been used as a shorthand for the process of obtaining, issuing, executing, and returning a warrant, as described in Rule 41"); In re Search of Yahoo, Inc., No. 07-3194, 2007 WL 1539971, at *5 (D. Ariz. May 21, 2007) (finding that "the phrase 'using the procedures described in' the Federal Rules remains ambiguous"). In light of this ambiguity, it is appropriate to look for guidance in the "statutory structure, relevant legislative history, [and] congressional purposes." Florida Light & Power Co. v. Lorion, 470 U.S. 729, 737 (1985); see Board of Education v. Harris, 444 U.S. 130, 140 (1979); Hall v. EarthLink Network, Inc., 396 F.3d 500, 504 (2d Cir. 2005).

B. Structure of the SCA

The SCA was enacted at least in part in response to a recognition that the Fourth Amendment protections that apply in the physical world, and especially to one's home, might not apply to information communicated through the internet.

> Absent special circumstances, the government must first obtain a search warrant based on probable cause before searching a home for evidence of crime. When we use a computer network such as the Internet, however, a user does not have a physical "home," nor really any private space at all. Instead,

> a user typically has a network account consisting of a block of computer storage that is owned by a network service provider, such as America Online or Comcast. Although a user may think of that storage space as a "virtual home," in fact that "home" is really just a block of ones and zeroes stored somewhere on somebody else's computer. This means that when we use the Internet, we communicate with and through that remote computer to contact other computers. Our most private information ends up being sent to private third parties and held far away on remote network servers.
>
> This feature of the Internet's network architecture has profound consequences for how the Fourth Amendment protects Internet communications—or perhaps more accurately, how the Fourth Amendment may not protect such communications much at all.

See Kerr, A User's Guide at 1209-10 (footnotes omitted).

Accordingly, the SCA created "a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information." Id. at 1212. Because there were no constitutional limits on an ISP's disclosure of its customer's data, and because the Government could likely obtain such data with a subpoena that did not require a showing of probable cause, Congress placed limitations on the service providers' ability to disclose information and, at the same time, defined the means that the Government could use to obtain it. See id. at 1209-13.

In particular, the SCA authorizes the Government to procure a warrant requiring a provider of electronic communication service to disclose e-mail content in the provider's electronic storage. Although section 2703(a) uses the term "warrant" and refers to the use of warrant procedures, the resulting order is not a conventional warrant; rather, the order is a hybrid: part search warrant and part subpoena. It is obtained like a search warrant when an application is made to a neutral magistrate who issues the order only upon a showing of probable cause. On the other hand, it is executed like a subpoena in that it is served on the ISP in possession of the information and does not involve government agents entering the premises of the ISP to search its servers and seize the e-mail account in question.

This unique structure supports the Government's view that the SCA does not implicate principles of extraterritoriality. It has long been the law that a subpoena requires the recipient to produce information in its possession, custody, or control regardless of the location of that information. See Marc Rich & Co., A.G. v. United States, 707 F.2d 663, 667 (2d Cir. 1983) ("Neither may the witness resist the production of documents on the ground that the documents are located abroad. The test for production of documents is control, not location." (citations omitted)); Tiffany (NJ) LLC v. Qi Andrew, 276 F.R.D. 143, 147-48 (S.D.N.Y. 2011) ("If the party suboenaed has the practical ability to obtain the documents, the actual physical location of the documents—even if overseas—is immaterial."); In re NTL, Inc. Securities Litigation, 244 F.R.D. 179, 195 (S.D.N.Y. 2007); United Sates v. Chase Manhattan Bank, N.A., 584 F. Supp. 1080, 1085 (S.D.N.Y. 1984).

To be sure, the "warrant" requirement of section 2703(a) cabins the power of the government by requiring a showing of probable cause not required for a subpoena, but it does not alter the basic principle that an entity lawfully obligated to produce information must do so regardless of the location of that information.

This approach is also consistent with the view that, in the context of digital information, "a search occurs when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when it is copied by the hard drive or processed by the computer." Orin S. Kerr, Searches and Seizures in a Digital World, 119 Harv. L. Rev. 531, 551 (2005). In this case, no such exposure takes place until the information is reviewed in the United States, and consequently no extraterritorial search has occurred.

This analysis is not undermined by the Eighth Circuit's decision in United States v. Bach, 310 F.3d 1063 (8th Cir. 2002). There, in a footnote the court noted that "[w]e analyze this case under the search warrant standard, not under the subpoena standard. While warrants for electronic data are often served like subpoenas (via fax), Congress called them warrants and we find that Congress intended them to be treated as warrants." Id. at 1066 n.1. Given the context in which it was issued, this sweeping statement is of little assistance to Microsoft. The issue in Bach was whether the fact that a warrant for electronic information was executed by employees of the ISP outside the supervision of law enforcement personnel rendered the search unreasonable in violation of the Fourth Amendment. Id. at 1065. The court utilized the stricter warrant

standard for evaluating the reasonableness of the execution of a search, as opposed to the standard for executing a subpoena; this says nothing about the territorial reach of an SCA Warrant.

C. Legislative History

Although scant, the legislative history also provides support for the Government's position. When the SCA was enacted as part of the ECPA, the Senate report, although it did not address the specific issue of extraterritoriality, reflected an understanding that information was being maintained remotely by third-party entities:

> The Committee also recognizes that computers are used extensively today for the processing and storage of information. With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. For example, physicians and hospitals maintain medical files in offsite data banks, businesses of all sizes transmit their records to remote computers to obtain sophisticated data processing services. . . . [B]ecause it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection.

S. Rep. No. 99-541, at 3 (1986).

While the House report did address the territorial reach of the law, it did so ambiguously. Because the ECPA amended the law with respect to wiretaps, the report notes:

> By the inclusion of the element "affecting (affects) interstate or foreign commerce" in these provisions the Committee does not intend that the Act regulate activities conducted outside the territorial United States. Thus, insofar as the Act regulates the "interception" of communications, for example it . . . regulates only those "interceptions" conducted within the territorial United States. Similarly, the controls in Section 201 of the Act [which became the SCA] regarding access to stored wire and electronic communications are intended to apply only to access within the territorial United States.

H.R. Rep. 99-647, at 32-33 (1986) (citations omitted). While this language would seem to suggest that information stored abroad would be beyond the purview of the SCA, it remains ambiguous for two reasons. First, in support of its observation that the ECPA does not regulate activities outside the United States, the Committee cited Stowe v. DeVoy, 588 F.2d 336 (2d Cir. 1978). In that case, the Second Circuit held that telephone calls intercepted in Canada by Canadian authorities were admissible in a criminal proceeding even if the interception would have violated Title III of the Omnibus Crime Control Act of 1968 if it had occurred in the Untied States or been performed by United States officials. Id. at 340-41. This suggests that Congress was addressing not the reach of government authority, but rather the scope of the individual rights created by the ECPA. Second, in referring to "access" to stored electronic communications, the Committee did not make clear whether it meant access to the location where the electronic data was stored or access to the location of the ISP in possession of the data.

Additional evidence of congressional intent with respect to this latter issue can be gleaned from the legislative history of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the "Patriot Act"). Section 108 of the Patriot Act provided for nationwide service of search warrants for electronic evidence. The House Committee described the rationale for this as follows:

> Title 18 U.S.C. § 2703(a) requires a search warrant to compel service providers to disclose unopened e-mails. This section does not affect the requirement for a search warrant, but rather attempts to address the investigative delays caused by the cross-jurisdictional nature of the Internet. Currently, Federal Rules of Criminal Procedure 41 requires that the "warrant" be obtained "within the district" where the property is located. An investigator, for example, located in Boston who is investigating a suspected terrorist in that city, might have to seek a suspect's electronic e-mail from an Internet service provider (ISP) account located in California. The investigator would then need to coordinate with agents, prosecutors and judges in the district in California where the ISP is located to obtain the warrant to search. These time delays could be devastating to an investigation, especially where additional criminal or terrorist acts are planned.
>
> Section 108 amends § 2703 to authorize the court with jurisdiction over the investigation to issue the warrant directly, without requiring the intervention of its counterpart in the district where the ISP is located.

H.R. Rep. 107-236(I), at 58 (2001). This language is significant, because it equates "where the property is located" with the location of the ISP, not the location of any server. See In re Search of Yahoo, Inc., 2007 WL 1539971, at *4 ("Commentators have suggested that one reason for the amendments effected by Section 220 of the Patriot Act was to alleviate the burden placed on federal district courts in the Eastern District of Virginia and the Northern District of California where major internet service providers [] AOL and Yahoo, respectively, are located.") (citing, inter alia, Patricia L. Bellia, Surveillance Law Through Cyberlaw's Lens, 72 Geo. Wash. L. Rev. 1375, 1454 (2004)).

Congress thus appears to have anticipated that an ISP located in the United States would be obligated to respond to a warrant issued pursuant to section 2703(a) by producing information within its control, regardless of where that information was stored.[3]

D. Practical Considerations

If the territorial restrictions on conventional warrants applied to warrants issued under section 2703(a), the burden on the Government would be substantial, and law enforcement efforts would be seriously impeded. If this were merely a policy argument, it would be appropriately addressed to Congress. But it also pro-

---

[3] Suppose, on the contrary, that Microsoft were correct that the territorial limitations on a conventional warrant apply to an SCA warrant. Prior to the amendment effected by the Patriot Act, a service provider could have objected to a warrant issued by a judge in the district where the provider was headquartered on the basis that the information sought was stored on a server in a different district, and the court would have upheld the objection and quashed the subpoena. Yet, I have located no such decision.

vides context for understanding congressional intent at the outset, for it is difficult to believe that, in light of the practical consequences that would follow, Congress intended to limit the reach of SCA Warrants to data stored in the United States.

First, a service provider is under no obligation to verify the information provided by a customer at the time an e-mail account is opened. Thus, a party intending to engage in criminal activity could evade an SCA Warrant by the simple expedient of giving false residence information, thereby causing the ISP to assign his account to a server outside the United States.

Second, if an SCA Warrant were treated like a conventional search warrant, it could only be executed abroad pursuant to a Mutual Legal Assistance Treaty ("MLAT"). As one commentator has observed, "This process generally remains slow and laborious, as it requires the cooperation of two governments and one of those governments may not prioritize the case as highly as the other." Orin S. Kerr, The Next Generation Communications Privacy Act, 162 U. Penn. L. Rev. 373, 409 (2014). Moreover, nations that enter into MLATs nevertheless generally retain the discretion to decline a request for assistance. For example, the MLAT between the United States and Canada provides that "[t]he Requested State may deny assistance to the extent that . . . execution of the request is contrary to its public interest as determined by its Central Authority." Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-Can., March 18, 1985, 24 I.L.M. 1092 ("U.S.-Can. MLAT"), Art. V(1). Similarly, the MLAT between the United States and the United Kingdom allows the Requested State to deny assis-

tance if it deems that the request would be "contrary to important public policy" or involves "an offense of a political character." Treaty on Mutual Legal Assistance in Criminal Matters, U.S.-U.K., Jan. 6, 1994, S. Treaty Doc. No. 104-2 ("U.S.-U.K. MLAT"), Art. 3(1)(a) & (c)(i). Indeed, an exchange of diplomatic notes construes the term "important public policy" to include "a Requested Party's policy of opposing the exercise of jurisdiction which is in its view extraterritorial and objectionable." Letters dated January 6, 1994 between Warren M. Christopher, Secretary of State of the United States, and Robin W. Renwick, Ambassador of the United Kingdom of Great Britain and Northern Ireland (attached to U.S.-U.K. MLAT). Finally, in the case of a search and seizure, the MLAT in both of these examples provides that any search must be executed in accordance with the laws of the Requested Party. U.S.-Can. MLAT, Art. XVI(1); U.S.-U.K. MLAT, Art. 14(1), (2). This raises the possibility that foreign law enforcement authorities would be required to oversee or even to conduct the acquisition of information from a server abroad.

Finally, as burdensome and uncertain as the MLAT process is, it is entirely unavailable where no treaty is in place. Although there are more than 60 MLATs currently in force, Amy E. Pope, Lawlessness Breeds Lawlessness: A Case for Applying the Fourth Amendment to Extraterritorial Searches, 65 Fla. L. Rev. 1917, 1931 (2013), not all countries have entered into such agreements with the United States. Moreover, Google has reportedly explored the possibility of establishing true "offshore" servers: server farms located at sea beyond the territorial jurisdiction of any nation. Steven R. Swanson, Google Sets Sail: Ocean-Based Server

Farms and International Law, 43 U. Conn. L. Rev. 709, 716-18 (2011). Thus, under Microsoft's understanding, certain information within the control of an American service provider would be completely unavailable to American law enforcement under the SCA.[4]

The practical implications thus make it unlikely that Congress intended to treat a Section 2703(a) order as a warrant for the search of premises located where the data is stored.

E. Principles of Extraterrioriality

The presumption against territorial application

> provides that "[w]hen a statute gives no clear indication of an extraterritorial application, it has none, Morrison v. National Australia Bank Ltd., 561 U.S. 247, __, 130 S. Ct. 2869, 2878 (2010), and reflect the "presumption that United States law governs domestically but does not rule the world," Microsoft Corp. v. AT & T Corp., 550 U.S. 437, 454 (2007).

Kiobel v. Royal Dutch Petroleum Co., __U.S.__, __, 133 S. Ct. 1659, 1664 (2013). But the concerns that animate the presumption against extraterritoriality are simply not present here: an SCA Warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data are stored. At least in this

---

[4] Non-content information, opened e-mails, and unopened emails stored more than 180 days could be obtained, but only by means of a subpoena with notice to the target; unopened e-mails stored less than 180 days could not be obtained at all.

instance, it places obligations only on the service provider to act within the United States. Many years ago, in the context of sanctioning a witness who refused to return from abroad to testify in a criminal proceeding, the Supreme Court observed:

> With respect to such an exercise of authority, there is no question of international law, but solely of the purport of the municipal law which establishes the duty of the citizen in relation to his own government. While the legislation of the Congress, unless the contrary intent appears, is construed to apply only within the territorial jurisdiction of the United States, the question of its application, so far as citizens of the United States are concerned, is one of construction, not of legislative power.

Blackmer v. United States, 284 U.S. 421, 437 (1932) (footnotes omitted). Thus, the nationality principle, one of the well-recognized grounds for extension of American criminal law outside the nation's borders, see Marc Rich, 707 F.2d at 666 (citing Introductory Comment to Research on International Law, Part II, Draft Convention on Jurisdiction With Respect to Crime, 29 Am. J. Int'l Law 435, 445 (Supp. 1935)), supports the legal requirement that an entity subject to jurisdiction in the United States, like Microsoft, may be required to obtain evidence from abroad in connection with a criminal investigation.

The cases that Microsoft cites for the proposition that there is no authority to issue extraterritorial warrants are inapposite, since these decisions refer to conventional warrants. For example, in United States v. Odeh, 552 F.3d 157 (2d Cir. 2008), the Second Circuit noted that "seven justices of the Supreme Court [in

United States v. Verdugo-Urquidez, 494 U.S. 259 (1990)] endorsed the view that U.S. courts are not empowered to issue warrants for foreign searches," id. at 169, and found that "it is by no means clear that U.S. judicial officers could be authorized to issue warrants for overseas searches," id. at 171. But Odeh involved American law enforcement agents engaging in wiretapping and searching a residence in Kenya. Id. at 159-60. The court held that while the Fourth Amendment's proscription against unreasonable search and seizure would apply in such circumstances, the requirement of a warrant would not. Id. at 169-71. Similarly, in Verdugo-Urquidez, the Supreme Court held that a Mexican national could not challenge, on Fourth Amendment grounds, the search of his residence in Mexico by American agents acting without a warrant. 494 U.S. at 262-63, 274-75; id. at 278 (Kennedy, J., concurring); id. at 279 (Stevens, J., concurring). Those cases are not applicable here, where the requirement to obtain a section 2703(a) order is grounded in the SCA, not in the Warrant Clause.

Nor do cases relating to the lack of power to authorize intrusion into a foreign computer support Microsoft's position. In In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753 (S.D. Tex. 2013), the court rejected the Government's argument that data surreptitiously seized from a computer at an unknown location would be "located" within the district where the agents would first view it for purposes of conforming to the territorial limitations of Rule 41. Id. at 756-57. But there the Government was not seeking an SCA Warrant.

> The Government [did] not seek a garden-variety search warrant. Its application request[ed] authorization to surreptitiously install data extraction software on the Target Computer. Once installed, the software [would have] the capacity to search the computer's hard drive, random access memory, and other storage media; to activate the computer's built-in camera; to generate latitude and longitude coordinates for the computer's location; and to transmit the extracted data to FBI agents within this district.

Id. at 755. "In other words, the Government [sought] a warrant to hack a computer suspected of criminal use." Id. Though not "garden-variety," the warrant requested there was conventional: it called for agents to intrude upon the target's property in order to obtain information; it did not call for disclosure of information in the possession of a third party. Likewise, in United States v. Gorshkov, No. CR 00-550, 2001 WL 1024026 (W.D. Wash. May 23, 2001), government agents seized a computer in this country, extracted a password, and used it to access the target computer in Russia. Id. at *1. The court characterized this as "extraterritorial access" to the Russian computer, and held that "[u]ntil the copied data was transmitted to the United States, it was outside the territory of this country and not subject to the protections of the Fourth Amendment." Id. at *3. But this case is of even less assistance to Microsoft since the court did not suggest that it would have

been beyond a court's authority to issue a warrant to accomplish the same result.[5]

Perhaps the case that comes closest to supporting Microsoft is Cunzhu Zheng v. Yahoo! Inc., No. C-08-1068, 2009 WL 4430297 (N.D. Cal. Dec. 2, 2008), because at least it deals with the ECPA. There, the plaintiffs sought damages against an ISP on the ground that it had provided user information about them to the People's Republic of China (the "PRC") in violation of privacy provisions of the ECPA and particularly of the SCA. Id. at *1. The court found that "the alleged interceptions and disclosures occurred in the PRC," id. at *4, and as a result, dismissed the action on the ground that "[p]laintiffs point to no language in the ECPA itself, nor to any statement in the legislative history of the ECPA, indicating Congress intended that the ECPA . . . apply to activities occurring outside the United States," id. at *3. But this language, too, does not advance Microsoft's cause. The fact that protections against "interceptions and disclosures" may not apply where those activities take place abroad hardly indicates that Congress intended to limit

---

[5] Microsoft argues that the Government itself recognized the extraterritorial nature of remote computer searches when it sought an amendment to Rule 41 in 2013. See Letter from Mythili Raman, Acting Assistant Attorney General, Criminal Division to Hon. Reena Raggi, Chair, Advisory Committee on Criminal Rules (Sept. 18, 2013) ("Raman Letter") at 4-5 , available at http://uscourts.gov/uscourts/RulesAndPolicies/. But the proposed amendment had nothing to do with SCA Warrants directed to service providers and, rather, was intended to facilitate the kind of "warrant to hack a computer" that was quashed in In re Warrant to Search a Target Computer at Premises Unknown; indeed, the Government explicitly referred to that case in its proposal. Raman Letter at 2.

the ability of law enforcement agents to obtain account information from domestic service providers who happen to store that information overseas.

Conclusion

Even when applied to information that is stored in servers abroad, an SCA Warrant does not violate the presumption against extraterritorial application of American law. Accordingly, Microsoft's motion to quash in part the warrant at issue is denied.

SO ORDERED.

/s/ JAMES C. FRANCIS IV
JAMES C. FRANCIS IV
UNITED STATES MAGISTRATE JUDGE

Dated: New York, New York
Apr. 25, 2014

Copies mailed this date:

Guy Petrillo, Esq.
Nelson A. Boxer, Esq.
Petrillo Klein & Boxer LLP
655 Third Ave.
New York, NY 10017

Nancy Kestenbaum, Esq.
Claire Catalano, Esq.
Covington & Burling LLP
The New York Times Building
620 Eighth Ave.
New York, NY 10018-1405

James M. Garland, Esq.
Alexander A. Berengaut, Esq.
Covington & Burling LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004-2401

Lorin L. Reisner, Esq.
Justin Anderson, Esq.
Serrin Turner, Esq.
Assistant U.S. Attorneys
One St. Andrew's Plaza
New York, NY 10007

APPENDIX C

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

No. 13 MJ 2814

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

New York, N.Y.
July 31, 2014
10:45 a.m.

Before: HON. LORETTA A. PRESKA, District Judge

APPEARANCES

PREET BHARARA
United States Attorney
for the Southern District of New York

JUSTIN ANDERSON
SERRIN TURNER
Assistant United States Attorneys

ORRICK, HERRINGTON & SUTCLIFFE
Attorneys for Microsoft
E. JOSHUA ROSENKRANZ
ROBERT E. LOEB
BRIAN P. GOLDMAN

PETRILLO KLEIN & BOXER
Attorneys for Microsoft
GUY PETRILLO

COVINGTON & BURLING
Attorneys for Microsoft
JAMES GARLAND
NANCY KESTENBAUM

* * * * *

[68] * * * THE COURT: Excellent. Give me two seconds, counsel.

I'm well aware of the requirement here of conducting a de novo review of the memorandum and order issued by Judge Francis. I have done that with the assistance of your very excellent briefing and arguments.

Having done that, I adopt the memorandum and order of Judge Francis. Today with your assistance, we have uncovered, [69] in my view, additional examples of why the structure, language, legislative history, Congressional knowledge of precedent, including the Bank of Nova Scotia doctrine, all lead to the conclusion that Congress intended in this statute for ISPs to produce information under their control, albeit stored abroad, to law enforcement in the United States. As Judge Francis found, it is a question of control, not a question of the location of that information.

The result of that finding is that the production of that information is not an intrusion on the foreign sovereign. It is incidental at best.

To the issue of the concerns of the foreign sovereign, in my view, the restatement Section 442(1)(a) is dispositive in that it states "A court or agency in the United States, when authorized by statute or rule of court" is empowered to "order a person subject to its

jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States."

That's precisely what is required here. And accordingly, I agree with Judge Francis that this is not an extraterritorial application of United States law.

In my view, also, the argument that the documents are not Microsoft's documents but the documents of its customers has been waived because it was not argued below.

[70]

In sum, the magistrate judge's memorandum and order is affirmed.

Counsel, thank you again for your excellent briefing and quite enjoyable arguments. * * *

APPENDIX D

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

No. M9-150/ 13-MJ-2814

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

[Filed: Aug. 12, 2014]

ORDER

LORETTA A. PRESKA, Chief United States District Judge:

This order confirms that immediately following oral argument on July 31, 2014, for the reasons set forth on the record, the Court affirmed the decision of Magistrate Judge James C. Francis IV dated April 25, 2014 [dkt. no. 5].

SO ORDERED.

Dated: New York, New York
Aug. 11, 2014

/s/ LORETTA A. PRESKA
LORETTA A. PRESKA
Chief United States District Judge

APPENDIX E

UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

Case Nos. 13-MAG-2814; M9-150

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

Sept. 8, 2014

ORDER

In accord with the parties' joint stipulation, and to permit prompt appellate review of this Court's July 31 ruling, this Court holds Microsoft Corporation in contempt for not complying in full with the Warrant, and imposes no other sanctions at this time. The Government may seek sanctions in the case of (a) materially changed circumstances in the underlying criminal investigation, or (b) the Second Circuit's issuance of the mandate in the appeal, if this Court's order is affirmed and Microsoft continues not to comply with it.

SO ORDERED.

Dated: Sept. 8, 2014
New York, New York

/s/ LORETTA A. PRESKA
LORETTA A. PRESKA
Chief United States District Judge

CERTIFICATE OF SERVICE

Justin Anderson affirms, under penalty of perjury, that he is employed in the Office of the United States Attorney for the Southern District of New York, and that, on today's date, he caused a copy of this submission to be served by this Court's electronic filing system on counsel of record in this matter.

Dated: Sept. 4, 2014
New York, New York

/s/ JUSTIN ANDERSON
JUSTIN ANDERSON
Assistant United States Attorney
Tel: (212) 637-1035

APPENDIX F

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

No. 14-2985

IN THE MATTER OF A WARRANT TO SEARCH A CERTAIN E-MAIL ACCOUNT CONTROLLED AND MAINTAINED BY MICROSOFT CORPORATION

MICROSOFT CORPORATION, APPELLANT

v.

UNITED STATES OF AMERICA, APPELLEE

Jan. 24, 2017

ORDER

Following disposition of this appeal, an active judge of the Court requested a poll on whether to rehear the case *en banc*.* A poll having been conducted and there being no majority favoring *en banc* review, rehearing *en banc* is hereby **DENIED**.

Susan L. Carney, *Circuit Judge*, concurs by opinion in the denial of rehearing *en banc*.

The following active judges were recused from participating in the poll: Rosemary S. Pooler, Debra Ann Livingston, and Raymond J. Lohier, Jr.

Dennis Jacobs, *Circuit Judge*, joined by José A. Cabranes, Reena Raggi, and Christopher F. Droney, *Circuit Judges*, dissents by opinion from the denial of rehearing *en banc*.

José A. Cabranes, *Circuit Judge*, joined by Dennis Jacobs, Reena Raggi, and Christopher F. Droney, *Circuit Judges*, dissents by opinion from the denial of rehearing *en banc*.

Reena Raggi, *Circuit Judge*, joined by Dennis Jacobs, José A. Cabranes, and Christopher F. Droney, *Circuit Judges*, dissents by opinion from the denial of rehearing *en banc*.

Christopher F. Droney, *Circuit Judge*, joined by Dennis Jacobs, José A. Cabranes, and Reena Raggi, *Circuit Judges*, dissents by opinion from the denial of rehearing *en banc*.

FOR THE COURT:

CATHERINE O'HAGAN WOLFE, CLERK

SUSAN L. CARNEY, *Circuit Judge*, concurring in the order denying rehearing *en banc*:

The original panel majority opinion, *see Microsoft Corp. v. United States*, 829 F.3d 197 (2d Cir. 2016), fully explains why quashing the government's warrant is called for by Supreme Court precedent on extraterritoriality and the text of the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701 *et seq.* Because the panel opinions did not include a dissent, however, I write again, briefly, to respond with respect to several points raised during our Court's consideration of whether to grant the government's petition for *en banc* review and reflected in the dissents from denial of rehearing.[1]

The theme running through the government's petition and the dissents is the concern that, by virtue of the result the panel reached, U.S. law enforcement will less easily be able to access electronic data that a magistrate judge in the United States has determined is probably connected to criminal activity.[2] My panel

---

[1] Judges Lynch and Bolden, who comprised the rest of the panel that heard this appeal, are not eligible to participate in deciding whether to rehear this case *en banc* because they are, respectively, a judge who entered senior status not long before the *en banc* poll was requested and a district judge sitting by designation. *See* 28 U.S.C. § 46(c) (limiting *en banc* voting to "the circuit judges of the circuit who are in regular active service").

[2] In this regard, it bears noting that an SCA section not at issue in this case, 18 U.S.C. § 2702(b)(8), authorizes "[a] provider . . . [to] divulge the contents of a communication . . . to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency," bypassing the warrant procedures of § 2703. Another section gives a provider immunity from civil liability for a

colleagues and I readily acknowledge the gravity of this concern. But the SCA governs this case, and so we have applied it, looking to the statute's text and following the extraterritoriality analysis of *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010). We recognize at the same time that in many ways the SCA has been left behind by technology. It is overdue for a congressional revision that would continue to protect privacy but would more effectively balance concerns of international comity with law enforcement needs and service provider obligations in the global context in which this case arose.[3]

Before going further, it is worth pointing out what is *not* at issue in this appeal. First, it is common ground that Congress did not intend for the SCA's warrant procedures to apply extraterritorially. *See* Gov't Pet. for Reh'g 11. Second, although the panel majority determined that the SCA's focus lies on protecting user privacy, this determination was made under the second part of the extraterritoriality analysis set forth as a canon of construction in *Morrison* and recently developed further in *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090 (2016). *See RJR Nabisco*, 136 S. Ct. at 2101 ("If the statute is not extraterritorial, then at the second step we determine whether the case

---

voluntary production of content made "in accordance with . . . [a] statutory authorization . . . under this chapter." 18 U.S.C. § 2703(e). The panel expressed no opinion on the use of these subsections, nor has it been suggested that the exigent circumstances of a "danger of death or serious physical injury" are presented here.

[3] This is a fact well appreciated by the Members of Congress who have introduced a bill proposing related amendments. *See* International Communications Privacy Act, S. 2986, H.R. 5323, 114th Cong. (2016).

involves a domestic application of the statute, and we do this by looking to the statute's "focus.'"). Our "focus" analysis did not turn on privacy protections independently derived from the Fourth Amendment. Nor did we express or imply a view about how Congress *may* permissibly legislate to enable the government to reach data stored abroad and under the control of U.S. companies; our reading of the SCA did no more than adhere to the dictates of *Morrison* in construing the SCA. Finally, since the instrument was issued by a neutral magistrate judge upon a showing of probable cause, no one disputes that the Microsoft warrant has satisfied the most stringent privacy protections our legal system affords.

Accordingly, the dispositive question in the case, as we see it, might be framed as whether Microsoft's execution of the warrant to retrieve a private customer's electronic data, stored on its servers in Ireland, would constitute an extraterritorial application of the SCA in light of the statute's "focus," determined in accordance with *Morrison* and *RJR Nabisco*. Again, this is a question of statutory construction. And, unsurprising in light of the need for an extraterritoriality analysis, it requires consideration of the concerns of sovereignty and international comity.

The panel majority concluded that "the relevant provisions of the SCA focus on protecting the privacy of the content of a user's stored electronic communications." *Microsoft*, 829 F.3d at 217. The concurring opinion noted the difficulty in determining a statute's "focus" under *Morrison*, but agreed that in the absence of any evidence that Congress intended the SCA to reach electronic data stored abroad by a service pro-

vider (and relating potentially to a foreign citizen), the effect of the government's demand here impermissibly fell beyond U.S. borders and therefore the Microsoft warrant should be quashed. *Id.* at 230-31 (Lynch, *J.*, concurring).

Guided by our determination of the statute's focus and looking at the text of the SCA itself, the panel majority read the statute to treat the locus of the SCA's privacy protections as at the place of data storage. As further detailed in the majority opinion, this conclusion comports with the SCA's reliance on the fact and form of content storage as predicates to its various provisions, as well as its use of the term of art "warrant" and its requirement of compliance with Federal Rule of Criminal Procedure 41, "Search and Seizure"—features usually associated with physical access. *See, e.g.*, 18 U.S.C. § 2701(a) (prohibiting access to "facilit[ies]" where electronic communications are stored); *id.* § 2702(a)(1)-(2) (prohibiting disclosure of communications "while in electronic storage" or "which [are] carried or maintained" by an electronic communication service); *id.* § 2703(a) (imposing warrant procedures on electronic communications that are "in electronic storage in an electronic communications system for one hundred and eighty days or less"). We noted that the statute uses "[t]he circumstances in which the communications have been stored . . . as a proxy for the intensity of the user's privacy interests, dictating the stringency of the procedural protection they receive." *Microsoft*, 829 F.3d at 217. We also noted that § 2701, by proscribing unauthorized access to storage facilities, not only limits disclosure but also "shelters the communications' integrity." *Id.* at 218. Because the electronic communications to be accessed and disclosed pursuant to the

Microsoft warrant are stored in a Dublin datacenter, we reasoned, the execution of the warrant would have its effect when the service provider accessed the data in Ireland, an extraterritorial application of the SCA.[4]

Characterizing the statute's focus differently, as resting on "disclosure," and offering a detailed recitation of the available statutory support for that conclusion,[5] the dissents argue primarily that the SCA's

---

[4] This approach, in which we considered several numbered sections of the SCA, is not inconsistent with *RJR Nabisco*. Rather than requiring a provision-by-provision analysis in every instance, as the government and some of the dissenters suggest in the context of their "focus" analysis, *see post* at 2 (Droney, *J.*, dissenting from the denial of reh'g *en banc*), *RJR Nabisco* involved looking at the expressed congressional intent with regard to the separately-enacted RICO predicate statutes, one by one, in the context of an overarching structure—that is, RICO. The panel majority here saw the SCA's relevant provisions, essentially enacted of a piece, as reflecting a single congressional expression with respect to extraterritorial application—a statutory circumstance quite different from the one addressed in *RJR Nabisco*.

[5] In support of their position my dissenting colleagues contend, as does the government, that an SCA warrant functions more like a subpoena than a traditional warrant and should be treated accordingly as reaching all documents under the control of the instrument's recipient. *See post* at 7 n.19 (Cabranes, *J.*, dissenting from the denial of reh'g *en banc*); *id.* at 1 (Jacobs, *J.*, dissenting from the denial of reh'g *en banc*). The SCA does not address a potential extraterritorial application of the instrument issued under § 2703—indeed it is unlikely, in view of the historical context, that Congress could have anticipated such an application, much less weighed domestic law enforcement interests against countervailing concerns with international comity. In light of the importance of these interests, it seems a stretch to conclude that we should read Congress's deliberate choice of the term "warrant" to reflect a concurrent intention to incorporate into the statute, without explicit mention, a body of case law addressing not warrants, but grand

effect occurs at the place of disclosure, on U.S. soil.[6] Thus, so long as (1) the warrant is served in the United

---

jury subpoenas. *Cf. id.* at 7 n.19 (Cabranes, *J.*, dissenting from the denial of reh'g *en banc*) (citing *Marc Rich & Co. v. United States*, 707 F.2d 663 (2d Cir. 1983)). Even the territorial reach of subpoenas is not an easy determination, in light of the many interests that courts must balance when addressing discovery that has foreign aspects. *See, e.g.*, Restatement (Third) of the Foreign Relations Law of the United States § 442(1)(c) (listing several factors courts "should take into account" when deciding whether to order production of information located abroad). Some of my dissenting colleagues also emphasize that the customer data at issue here is already in Microsoft's possession. *See post* at 9-11 (Raggi, *J.*, dissenting from the denial of reh'g *en banc*). The SCA constrains a service provider's use of that "possession," recognizing the provider's role as an intermediary between the customer who created the content and third parties. Thus, it distinguishes in its level of privacy protections between customers' substantive content and the administrative data that a provider maintains for its own purposes with respect to those customers. *See* 18 U.S.C. § 2703(c) (distinguishing between "contents of communications" and information such as a customer's name, address, and service details).

[6] As explored further below, although the SCA is broadly focused on privacy, it does address disclosure, most particularly in § 2702, as an exception to its general rule of maintaining the confidentiality of customer content. *See post* at 10-13 (Cabranes, *J.*, dissenting from the denial of reh'g *en banc*). The panel majority read the SCA to focus foremost on protecting user privacy by controlling access to stored communications—controls that apply even to service providers (if, for example, an employee exceeded his or her authorization with respect to stored data). To the extent that the majority opinion "raises concerns about the extraterritorial reach of *protections* from unlawful access and disclosures afforded by sections 2701 and 2702," *id.* at 14 n.36 (Cabranes, *J.*, dissenting from the denial of reh'g *en banc*) (emphasis added), one might take some comfort from the privacy laws of other countries that would apply to servers on their territory (and the significant incentives for service providers to guard against unauthorized intrusion).

States on a provider doing business in the United States, and (2) the provider can access the user's content electronically from the United States, extraterritoriality need not even be considered.[7] Since the warrant recipient here is Microsoft, a U.S. corporation (though the reasoning would apply equally well to a foreign provider who is sufficiently present in the United States), and the data is accessible and producible by Microsoft to the U.S. government in the United States, no more is needed to enforce the warrant. The inquiry stops there.

The panel majority rejected this position, and a few reflections illustrate why we were correct to do so. First: The position of the government and the dissenters necessarily ignores situations in which the effects outside the United States are less readily dismissed, whichever label is chosen to describe the "focus" of the statute. For example, under the dissents' reasoning (as we understand it), the SCA warrant is valid when

---

More importantly, however, the dissents' concerns about the reach outside the United States of the protections established by the statute provide yet another reason for congressional overhaul of the SCA.

[7] Taken to its logical conclusion, the dissents' focus on the place of disclosure to the exclusion of other factors would mean that, so long as the requested data is to be disclosed to the government within the United States, the SCA has only domestic application. But because, presumably, data demanded by the United States government under the SCA can *always* be expected to be disclosed to the government in the United States absent special circumstances, no application of the SCA's data disclosure procedures would be extraterritorial. At a time when U.S. companies, to their great credit, provide electronic communications services to customers resident around the globe, this observation suggests the demerits of the analysis.

(1) it is served in the United States on a branch office of an Irish service provider, (2) it seeks content stored in Ireland but accessible at the U.S. branch, (3) the account holding that content was opened and established in Ireland by an Irish citizen, (4) the disclosure demanded by the warrant would breach Irish law, and (5) U.S. law enforcement could request the content through the MLAT process.[8] This hardly seems like a "domestic application" of the SCA. Rather, we find it difficult to imagine that the Congress enacting the SCA envisioned such an application, much less that it would not constitute the type of extraterritorial application with which *Morrison* was concerned. Indeed, calling such an application "domestic" runs roughshod over the concerns that undergird the Supreme Court's strong presumption against extraterritoriality, and suggests the flaw in an approach to the SCA that considers only

---

[8] As noted in the panel majority opinion, MLATs are Mutual Legal Assistance Treaties "between the United States and other countries, which allow signatory states to request one another's assistance with ongoing criminal investigations, including issuance and execution of search warrants." *Microsoft*, 829 F.3d at 221. The United States has entered into approximately 56 MLATs with foreign countries, including all member states of the European Union, and holds related Mutual Legal Assistance Agreements with others. *See id.* n.29; U.S. Dep't of State, *Treaties & Agreements*, https://www.state.gov/j/inl/rls/nrcrpt/2012/vol2/184110.htm. As the dissenters fairly point out, however, the United States lacks an MLAT relationship with many countries, and the MLAT process can be cumbersome. *See post* at 5 n.11 (Cabranes, *J.*, dissenting from the denial of reh'g *en banc*). In this case, the Republic of Ireland filed a brief *amicus curiae*, acknowledging its MLAT with the United States and representing its willingness "to consider, as expeditiously as possible, a request under the treaty." Br. *Amicus Curiae* Ireland 4, *Microsoft Corp. v. United States*, No. 14-2985 (2d Cir. December 2014).

disclosure. *See Morrison*, 561 U.S. at 269 (citing "probability of incompatibility with applicable laws of other countries" as signaling absence of congressional attention to extraterritorial application); *EEOC v. Arabian Am. Oil Corp.*, 499 U.S. 244, 248 (1991) (observing that presumption against extraterritoriality "serves to protect against unintended clashes between our laws and those of other nations").

Second: My dissenting colleagues take issue with the idea that "privacy" can have a territorial locus at all when it comes to electronic data, given the ease with which the data can be subdivided or moved across borders and our now familiar notion of data existing in the ephemeral "cloud." But, mundane as it may seem, even data subject to lightning recall has been stored somewhere, and the undisputed record here showed that the "somewhere" in this case is a datacenter firmly located on Irish soil.[9] *See Microsoft*, 829 F.3d at 220 n.28. (Fragmentation, an issue raised by the government in its petition and by the dissents here, was not present in the facts before the panel, and only further emphasizes the need for a modernized statute.) When

---

[9] Microsoft represents in the record that it stores data in different locations around the world not at whim, but for competitive commercial reasons: so that the data can be more quickly recalled for users based on proximity to their reported geographic locations. *See Microsoft*, 829 F.3d at 202. The record contains no basis for speculating that it has stored data in locations engineered to avoid an obligation to produce the data in response to law enforcement needs or to enable criminal activity to go undetected. Nor, although a customer could certainly do so, does the record suggest that the customer whose account is at issue falsely designated Ireland as its location to escape the reach of U.S. law enforcement. That customer could as well be a citizen of Ireland as of any other nation.

Congress passed the "*Stored* Communications Act" in 1986, the statute it enacted protected data by limiting access to the "facility" where the data is stored or through which electronic services are provided. 18 U.S.C. § 2701(a). It did not address the citizenship of the account holder, the nationality of the service provider, or any of the concerns that can be cited, legitimately, as relevant today to defining a sound policy concerning the privacy and disclosure of protected user content in a global setting. Nor have we been pointed to evidence suggesting that sovereigns have relinquished any claim to control over data physically stored within their boundaries. (Ireland certainly did not do so here in its submission *amicus curiae*.) Although the realities of electronic storage have widely outstripped what Congress envisioned in 1986, we are not so far from the context of the SCA that we can no longer apply it faithfully.

To connect these two points: Some of my dissenting colleagues, *see post* at 5 (Jacobs, *J.*, dissenting from the denial of reh'g *en banc*), like the panel, have noted potential concerns with reciprocity—that if the United States can direct a service provider with operations in the United States to access data of a foreign citizen stored in a foreign country, a foreign sovereign might claim authority to do the same and access data of a U.S. citizen stored in the United States, so long as the data would be disclosed abroad. If this concern holds any intuitive force, it does so only because the location of data storage *does* still have import, and therefore reaching across physical borders to access electronic data gives us pause when we are on the receiving end of the intrusion. It is for just this sort of reason that the government has entered into MLATs with other

sovereigns: to address mutual needs for law enforcement while respecting sovereign borders. And it is for just this sort of reason that the government has in other circumstances taken a position, somewhat in tension with the one it takes here, that courts should be particularly solicitous of sovereignty concerns when authorizing data to be collected in the United States but drawn from within the boundaries of a foreign nation. *See, e.g.*, Br. United States *Amicus Curiae* Opp'n Pet. Writ Cert. 8-21, *Arab Bank, PLC v. Linde*, No. 12-1485 (May 2014) (contending, in civil discovery context, that lower courts erred in "failing to accord sufficient weight to the foreign jurisdictions' interests in enforcing their bank secrecy laws").

Third, and finally: The exercise of selecting a "focus" and then determining its territorial locus highlights some of the difficulties inherent in applying the *Morrison* extraterritoriality analysis. Where the panel majority and the dissents diverge most sharply and meaningfully is on the better view of the legal consequences of the focus inquiry: *where*—for purposes of assessing extraterritoriality according to the Supreme Court's precedents—to locate the affected interest. Once we concluded that the statute focuses on protecting privacy, the panel majority had to assess further where privacy might be considered to be physically based—an elusive inquiry, at best. As noted, the dissents emphasize disclosure, and reason from that premise that the place of disclosure establishes whether the proposed application of the statute is domestic. But we saw the overarching goal of the SCA as protecting privacy and allowing only certain exceptions, of which limited disclosure in response to a warrant is one. Considerations of privacy and disclosure cannot be

divorced; they are two sides of the same coin. By looking past privacy and directly to disclosure, however, the dissents would move the "focus" of the statute to its exceptions, and away from its goal. The better approach, which in our estimation is more in keeping with the *Morrison* analysis and the SCA's emphasis on data storage, is one that looks to the step taken before disclosure—access—in determining privacy's territorial locus.

With a less anachronistic statute or with a more flexible armature for interpreting questions of a statute's extraterritoriality, we might well reach a result that better reconciles the interests of law enforcement, privacy, and international comity. In an analytic regime, for example, that invited a review of the totality of the relevant circumstances when assessing a statute's potential extraterritorial impact, we might be entitled to consider the residency or citizenship of the client whose data is sought, the nationality and operations of the service provider, the storage practices and conditions on disclosure adopted by the provider, and other related factors. And we can expect that a statute designed afresh to address today's data realities would take an approach different from the SCA's, and would be cognizant of the mobility of data and the varying privacy regimes of concerned sovereigns, as well as the potentially conflicting obligations placed on global service providers like Microsoft. As noted above, there is no suggestion that Congress could not extend the SCA's warrant procedures to cover the situation presented here, if it so chose.

These were not the statutory context and precedent available to the panel, however, nor would they be available to our Court sitting *en banc*. Under the circumstances presented to us, the Microsoft warrant was properly quashed.

DENNIS JACOBS, *Circuit Judge*, joined by JOSÉ A. CABRANES, REENA RAGGI, and CHRISTOPHER F. DRONEY, *Circuit Judges*, dissenting from the denial of rehearing in banc:

The United States has ordered Microsoft to provide copies of certain emails pursuant to the Stored Communications Act. A magistrate judge found probable cause to believe those emails contain evidence of a crime. (The instrument functions as a subpoena though the Act calls it a warrant.) A panel of this Court directed the district court to quash the warrant as an unlawful extraterritorial application of the Act. Now, in a vote split four-four, we decline to rehear the case in banc. I respectfully dissent from the denial.

I subscribe to the dissents of Judge Cabranes, Judge Raggi, and Judge Droney, which set out in detail the doctrinal basis for the right result in this appeal. I write separately to describe an approach that is perhaps more reductionist.

I

As all seem to agree, and as the government concedes, the Act lacks extraterritorial reach. However, no extraterritorial reach is needed to require delivery in the United States of the information sought, which is easily accessible in the United States at a computer terminal. The majority nevertheless undertakes to determine whether this case presents a forbidden extraterritorial application by first "look[ing] to the 'territorial events or relationships' that are the 'focus' of the relevant statutory provision." Majority Op., 829 F.3d at 216 (quoting *Mastafa v. Chevron Corp.*, 770 F.3d 170, 183 (2d Cir. 2014)). Oddly, the majority then holds that the

relevant "territorial" "focus" is user privacy. But privacy, which is a value or a state of mind, lacks location, let alone nationality.[1] Territorially, it is nowhere. Important as privacy is, it is in any event protected by the requirement of probable cause; so a statutory focus on privacy gets us no closer to knowing whether the warrant in question is enforceable.

Extraterritoriality need not be fussed over when the information sought is already within the grasp of a domestic entity served with a warrant. The warrant in this case can reach what it seeks because the warrant was served on Microsoft, and Microsoft has access to the information sought. It need only touch some keys in Redmond, Washington. If I can access my emails from my phone, then in an important sense my emails are in my pocket, notwithstanding where my provider keeps its servers.

The majority opinion relies on an implicit analogy to paper documents: "items" and "material" and "content" that are "located" and "stored and that the government seeks to "collect" and "import." But electronic data are not stored on disks in the way that books are stored on shelves or files in cabinets. Electronic "documents" are literally intangible: when we say they are stored on a disk, we mean they are encoded on it as a pattern. At stake in this case is not whether Microsoft can be compelled to import and deliver a disk (or anything else), but whether Microsoft can be compelled

---

[1] As Judge Lynch wrote in his panel concurrence, privacy "is an abstract concept with no obvious territorial locus," and the majority's conclusion therefore "does not really help us to distinguish domestic applications of the statute from extraterritorial ones." Concurring Op., 829 F.3d at 230 n.7.

to deliver information that is encoded on a disk in a server and that Microsoft can read.

The panel's approach is unmanageable, and increasingly antiquated. As explained in an article Judge Lynch cites in his concurrence (829 F.3d at 229): "[T]he very idea of online data being located in a particular physical 'place' is becoming rapidly outdated," because electronic "files [can] be fragmented and the underlying data located in many places around the world" such that the files "only exist in recognizable form when they are assembled remotely." Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 408 (2014). The underlying data can be fragmented or recombined, copied or transferred, for convenience or maintenance or economy —or (not incidentally) to evade the police. And all that can be done at the direction of the user or without the user's knowledge, and without a care for national boundaries, tariffs or postage. Nothing moves but information.

To enforce the warrant, there is no practical alternative to relying upon access, and no need to seek an alternative. We can conclude that warrants can reach what their recipients can deliver: if the recipient can access a thing here, then it can be delivered here; and if statutory and constitutional standards are met, it should not matter where the ones-and-zeroes are "stored."

Localizing the data in Ireland is not marginally more useful than thinking of Santa Claus as a denizen of the North Pole. Problems arise if one over-thinks the problem, reifying the notional: Where in the world

is a Bitcoin? Where in my DVR are the images and voices? Where are the snows of yesteryear?

II

The majority has found no indication that Congress considered in 1986 whether a warrant issued under the Act would reach data stored on servers outside the United States; and Judge Lynch's concurrence, having recognized the flaws in the majority opinion, calls on Congress to modernize the statute. I too would like to see Congress act, chiefly to consider certain ramifications, such as whether the United States might be vulnerable to reciprocal claims of access through local offices of American companies abroad. But we are not in a position to punt when it comes to construing a statute that either does or does not allow execution of a warrant in a case that is before us now. Holding, as the panel did, that the statute does not allow enforcement of this warrant is an interpretation of the statute, not a deferential bow to Congress. So though it would best if Congress could form a consensus on the issue, that preference is not a principle of statutory construction.

Nor can it matter how we would order legislative priorities (this would seem to be a bit down the list), or how much we would welcome bipartisan consideration of a bill that has not been enacted. Legislative proposals are myriad, and they fall as leaves. Come what may, we are left for now with the law as it is. The panel misconstrues it, and I would rehear the case in banc.

JOSÉ A. CABRANES, *Circuit Judge*, joined by DENNIS JACOBS, REENA RAGGI, and CHRISTOPHER F. DRONEY, *Circuit Judges*, dissenting from the order denying rehearing *en banc*:

An evenly-divided *en banc* court has declined to rehear a case that presents multiple questions of exceptional importance to public safety and national security.[1] I respectfully dissent.

The panel majority quashed a warrant issued under section 2703 of the Stored Communications Act ("SCA")[2] by a judicial officer of the United States upon a showing of probable cause. It erroneously concluded that the government's use of an SCA warrant to require a United States-based service "provider" (Microsoft) to disclose the contents of a customer's emails stored on servers located in Ireland was an extraterritorial application of the SCA.[3] The panel majority ignored the fact that Microsoft lawfully had possession of the emails; that Microsoft had access to the emails in the

---

[1] We have had occasion to observe that the decision to deny rehearing *en banc* "does not necessarily mean that a case either lacks significance or was correctly decided. Indeed, the contrary may be true. An oft-cited justification for voting *against* rehearing, perhaps counterintuitively, is that the case is '*too important* to *en banc*.'" *United States v. Taylor*, 752 F.3d 254, 256 (2d Cir. 2014) (quoting James L. Oakes, *Personal Reflections on Learned Hand and the Second Circuit*, 47 STAN. L. REV. 387, 392 (1995)) (emphasis in original). Accordingly, a reader should not give "any extra weight to a panel opinion in light of such a decision, inasmuch as the order denying rehearing may only reflect, for some judges, a general aversion to *en banc* rehearings or faith in the Supreme Court to remedy any major legal errors." *Id.* at 257.

[2] *See* 18 U.S.C. §§ 2701-12.

[3] *See* Majority Op. at 42.

United States; and that Microsoft's disclosure of the emails to the government would take place in the United States. In its unprecedented ruling, the panel majority has indisputably, and severely, restricted "an essential investigative tool used thousands of times a year [in] important criminal investigations around the country."[4] To top this off, the panel majority's decision does not serve any serious, legitimate, or substantial privacy interest.[5]

I.

The negative consequences of the panel majority's opinion are far reaching. It has substantially burdened the government's legitimate law enforcement efforts; created a roadmap for the facilitation of criminal activity; and impeded programs to protect the national security of the United States and its allies.[6]

---

[4] Petition for Rehearing and Rehearing En Banc ("En Banc Petition") 2-3. In just the second half of 2015, Google alone "received 3,716 warrants seeking data from a total of 9,412 accounts." *Id.* at 18.

[5] In his concurring opinion, Judge Lynch observes that despite Microsoft's suggestion that "this case involves a government threat to individual privacy. . . . uphold[ing] the warrant here would not undermine basic values of privacy as defined in the Fourth Amendment and in the libertarian traditions of this country." Concurring Op. at 1. As he explains, "the government complied with the most restrictive privacy-protecting requirements of the [SCA]. Those requirements are consistent with the highest levels of protection ordinarily required by the Fourth Amendment for the issuance of search warrants." *Id.* at 2.

[6] Judge Carney's opinion concurring in the order denying rehearing *en banc* does not dispute the fact that the panel majority's decision has put the safety and security of Americans at risk. Instead, in a footnote, the concurring opinion notes two sections of the SCA that it believes lessen the severity of these consequences.

First, as Judge Lynch's concurring opinion explains, the panel majority's holding affords "absolute" protection from disclosure to electronic communications stored abroad, regardless of whether they are controlled by a domestic service provider and are accessible from within the United States.[7] As a result, the government can "never obtain a warrant" that would require a service provider to turn over emails stored in servers located outside the United States, regardless of how "certain [the government] may be that [emails] contain evidence of criminal activity, and even if that criminal activity is a terrorist plot."[8]

Second, the panel majority's opinion has created a roadmap for even an unsophisticated person to use email to facilitate criminal activity while avoiding detection by law enforcement. The Microsoft customer targeted by the government's warrant in this case indicated to Microsoft when he signed up for its service that he

---

Ante at 1 n.2 (Carney, *J.*, concurring in the order denying reh'g *en banc*). The first section, 2702(b)(8), permits "[a] provider . . . [to] divulge the contents of a communication . . . to a government entity, *if the provider*, in good faith, believes that" there are exigent circumstances. *Id.* (quoting 18 U.S.C. § 2702(b)(8)) (emphasis added). The second section, 2703(e), "gives a provider immunity from civil liability for a voluntary production of content made 'in accordance with . . . [a] statutory authorization. . . .'" *Id.* at 2 n.2 (quoting 18 U.S.C. § 2703(e)). In asking us to entrust our national security to the good faith of internet service providers, I can only assume that the concurring opinion has some unstated reason for believing that Microsoft is just an atypically unpatriotic service provider and that other, more virtuous, service providers would never put their business interests ahead of public safety and national security.

[7] Concurring Op. at 4.

[8] *Id.* at 4-5.

resided in Ireland—a representation Microsoft took at face value.[9] Because Microsoft has a policy of "stor[ing] a customer's email information . . . at datacenters located near the physical location identified by the user as its own," Microsoft automatically stored his emails on its servers in Ireland—now safely beyond the reach of an SCA warrant.[10] Based on the panel majority's holding, a criminal who resides in the United States can now check the proverbial "box" informing Microsoft that he resides in another country when signing up for service—perhaps a country without a Mutual Legal Assistance Treaty ("MLAT") with the United States[11] —and thereby avoid having his emails disclosed to the government pursuant to an SCA warrant.

Third, the panel majority's decision has already led major service providers to reduce significantly their cooperation with law enforcement. The panel majority held that the physical location of a server containing a customer's emails determines whether an SCA warrant seeking the disclosure of those emails is an extraterritorial application of the SCA. However, electronic data storage is more complex and haphazard than the panel majority's holding assumes. Many service providers regularly "store different pieces of information

---

[9] Majority Op. at 8-9.

[10] *Id.*

[11] The United States has entered into MLATs with several countries, allowing parties to the treaty to request assistance with ongoing criminal investigations, including issuance and execution of search warrants. *See id.* at 41. However, many countries do not have MLATs with the United States, *e.g.*, Indonesia and Pakistan, and law enforcement cooperation with those countries is limited. *See* Gov't Br. 48-53 (describing the inefficiencies of the MLAT process as well as its ineffectiveness in certain circumstances).

for a single customer account in various datacenters at the same time, and routinely move data around based on their own internal business practices."[12] Still other providers are unable to determine "where particular data is stored or whether it is stored outside the United States."[13] Consequently, in an effort to apply the panel majority's confected holding to the technological realities of electronic data storage, major service providers are adopting restrictive disclosure policies that radically undermine the effectiveness of an SCA warrant.[14]

For example, Google will now disclose "only those portions of customer accounts stored in the United States at the moment the warrant is served."[15] Google's policy is particularly troubling because "the only [Google] employees who can access the entirety of a customer's account, including those portions momentarily stored overseas, are located in the United States."[16] As a result, law enforcement might never be able obtain data stored in Google servers abroad, even with the help of an MLAT.

Yahoo! has advised law enforcement that it "will not even preserve data located outside the United States in

---

[12] En Banc Petition 18-19

[13] *Id.*

[14] *See Id.* 17-19; see also Orin Kerr, *The Surprising Implications of the Microsoft/Ireland Warrant Case*, WASH. POST: THE VOLOKH CONSPIRACY (Nov. 29, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/29/thesurprising-implications-of-the-microsoftireland-warrant-case.

[15] En Banc Petition 19.

[16] *Id.*

response to a [s]ection 2703 request."[17] This policy, as the government points out in its En Banc Petition, creates "a risk that data will be moved or deleted before the United States can seek assistance from a foreign jurisdiction, much less actually serve a warrant and secure the data."[18]

II.

The baleful consequences of the panel's decision are compelled neither by the text of the statute nor by our precedent. The panel majority arrived at its damaging holding because it adopted a flawed reading of the SCA.

The second step of the two-step framework for analyzing extraterritoriality issues set forth in *Morrison v. National Australia Bank Ltd.*, 561 U.S. 247 (2010), and *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090 (2016), was the determinative issue in this case.[19]

---

[17] *Id.*

[18] *Id.*

[19] The first step of the extraterritorial analysis is "to determine whether the relevant statutory provision contemplates extraterritorial application." Majority Op. at 22 (citing *Morrison*, 561 U.S. at 262-65). Because the government conceded at oral argument that the SCA lacks extraterritorial application, *id.*, there is no need to pursue the point. To the extent the panel majority did so in a lengthy discussion of the SCA's use of the word "warrant" in section 2703, *see id.* at 25-31, which then informs its step-two "focus" analysis, it is appropriate to note concern with the reasoning.

The panel majority conflates SCA disclosure warrants with traditional search warrants. While the latter authorize government action as to *places*, the former authorize government action on *persons*. The fact that warrants generally do not authorize government searches of places outside the United States—a limitation grounded in respect for sovereignty, not privacy, *see, e.g.*, *The*

At step two, a court must "determine whether the case involves a domestic application of the statute," which "we do . . . by looking to the statute's "focus'" and by identifying where "the conduct relevant to the statute's focus occurred."[20] Here, the panel majority

---

Apollon, 22 U.S. (9 Wheat.) 362, 371 (1824) (Story, J.); Restatement (Third) of Foreign Relations Law § 432(2); *see also In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157, 167-72 (2d Cir. 2008)—does not support a conclusion that warrants are impermissibly applied extraterritorially when they compel persons within the United States to disclose property lawfully in their possession anywhere in the world. *Cf. Linde v. Arab Bank, PLC*, 706 F.3d 92, 109 (2d Cir. 2013) (Carney, J.) (observing that the Supreme Court has held that "the operation of foreign law 'do[es] not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that [law]." (quoting *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court*, 482 U.S. 522, 544 n. 29 (1987)). In that sense, a disclosure warrant is more akin to a subpoena, *see, e.g., Marc Rich & Co. A.G. v. United States*, 707 F.2d 663, 668-70 (2d Cir. 1983) (holding that persons in the United States can be required to retrieve subpoenaed material from abroad), *but* with the important added protection of a probable cause showing to a neutral magistrate. Thus, the panel majority is simply wrong in concluding that "a warrant protects *privacy* in a distinctly territorial way." Majority Op. at 26 (emphasis added). Warrants protect privacy through the Fourth Amendment requirement that they issue only upon probable cause. *See* Concurring Op. at 1-3.

By failing to distinguish between search warrants as to places and disclosure warrants directed to persons, and between sovereignty and privacy, the panel majority construes "warrant" as used in the SCA to yield the perverse result of affording greater privacy protection to foreign nationals and Americans who say they reside abroad than to resident United States citizens with respect to electronic communications in the lawful possession of a United States service provider.

[20] *RJR Nabisco*, 136 S. Ct. at 2101.

explained that the "focus" of the SCA is user privacy,[21] and in a single sentence, identified the location of the conduct relevant to that focus: "[I]t is our view that the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed—here, where it is seized by Microsoft, acting as an agent of the government."[22] Because the emails at issue were stored on a server in Ireland, the panel majority concluded that the warrant seeking the disclosure of those emails was an extraterritorial application of the SCA.[23] Not so.

---

[21] *See* Majority Op. at 32-39.

[22] *Id.* at 39. Judge Carney's opinion concurring in the order denying rehearing *en banc* reiterates the panel majority's conclusion —that, "the locus of the SCA's privacy protections [is] at the place of data storage"—but again provides little or no explanation for how or why the statutory language permits such a reading. *Ante* at 4 (Carney, *J.*, concurring in the order denying reh'g *en banc*). It offers only the sphinx-like explanation that "§ 2701, by proscribing unauthorized access to storage facilities, not only limits disclosure but also 'shelters the communications' integrity.'" *Id.* at 5 (quoting Majority Op. at 35). Conversely, and as the concurring opinion itself notes, those of us dissenting from the denial of *en banc* review "offer[] a detailed recitation of the available statutory support for [the] conclusion" that the conduct relevant to the SCA's focus occurs at the place of disclosure. *Id.* at 6.

[23] Judge Carney's *en banc* concurrence asserts that the panel majority's "reading of the SCA did no more than adhere to the dictates of *Morrison* in construing the SCA." *Ante* at 3 (Carney, *J.*, concurring in the order denying reh'g *en banc*). I disagree. Instead of locating support for its legal conclusion in the text or structure of the SCA, the concurring opinion, like the panel majority's opinion, fixates on its unsubstantiated belief that the warrant at issue here raises "concerns of sovereignty and international comity." *Id.* at 4. They both then conclude, based primarily on that misconception, that the warrant at issue must be an extrater-

Even if the "focus" of the SCA is user privacy, a plain reading of the statute makes clear that the conduct relevant to the SCA's "focus," and which the SCA seeks to regulate, is a provider's *disclosure* or *non-disclosure* of emails to third parties, not a provider's *access* to a customer's data. Here, Microsoft's disclosure of emails to the government would take place at its headquarters in the United States. Therefore, had the panel majority correctly identified the conduct relevant to the SCA's "privacy focus," it would have concluded that the warrant at issue was a domestic application of the SCA.[24]

---

ritorial application of the SCA. *Morrison*, however, does not permit a court to conclude that a particular application of a statute is extraterritorial simply because it believes that the application threatens international comity. Rather, step two of the *Morrison* framework directs courts to examine the statutory language. *See Morrison*, 561 U.S. at 266-67.

[24] According to the *en banc* concurrence, the panel majority considered and rejected my suggested holding partly because that holding "ignores situations in which the effects outside the United States are less readily dismissed." *Ante* at 8 (Carney, *J.*, concurring in the order denying reh'g *en banc*). As far as I understand it, the concurring opinion asserts the belief that the facts of this case are too sympathetic to my interpretation of the law and that only under alternative, entirely fictional, circumstances would the true menace of my position be revealed. It then devises a hypothetical warrant that purports to show how my suggested holding permits the authorization of warrants with too limited a nexus to the United States: an SCA warrant requiring a "United States . . . branch office of an Irish service provider" to disclose electronic information stored in Ireland but accessible in the United States that belonged to an account "opened and established in Ireland by an Irish citizen," the disclosure of which would breach Irish law. *Id.*

A brief examination of the text and structure of the SCA leads inexorably to the conclusion that the conduct relevant to the SCA's "privacy focus" is its regulation of *disclosures* by providers to third-parties. As the panel majority observes, "the first three sections of the SCA contain its major provisions."[25] The first of those sections, section 2701, addresses "[u]nlawful access to stored communications."[26] Section 2701 is the *only* major provision of the SCA to specifically limit *access* to customer communications. Although the panel majority fails to explain adequately why the "invasion of the customer's privacy takes place . . . where the customer's protected content is *accessed*,"[27] section 2701 is the only plausible textual basis for the panel majority's bizarre holding.

However, while section 2701 prohibits "[u]nlawful access" (most obviously hacking), it recognizes that providers have standing authority to *access* a customer's

---

This hypothetical is too clever by half. In attempting to construct the most shocking warrant conceivable, the concurring opinion omits two critical facts, both of which are required under my understanding of the law. First, a judicial officer of the United States would have to issue the warrant upon a finding of probable cause to believe that the information being sought was related to criminal activity occurring within the United States. Second, the provider would have to disclose the targeted information to the government inside the United States. Thus, if all of the conditions necessary for a valid SCA warrant are satisfied, there is no basis for concluding that even Judge Carney's imagined warrant, not to mention the warrant at issue, is an extraterritorial application of the SCA.

[25] *Id.* at 35; *see* 18 U.S.C. §§ 2701-03

[26] 18 U.S.C. § 2701.

[27] Majority Op. at 39 (emphasis added).

electronic communications.[28] In fact, section 2701(c) expressly exempts from its restrictions on *access* "conduct authorized . . . by the person or entity providing a wire or electronic communications service," *i.e.*, the provider.[29] It is unreasonable, therefore, for the panel majority to conclude that a provider's lawful access to a customer's emails is the conduct relevant to the SCA's "privacy focus."[30]

On the other hand, section 2702 expressly prohibits, with some exceptions, a provider from "*disclos[ing]*" a customer's communications.[31] For example, section 2702(a) sets forth three "[p]rohibitions" that must be followed by servicer providers like Microsoft.[32] Each prohibition states that the provider "shall not knowingly *divulge*" certain information, such as the contents of a communication, unless an exception in subsection (b) or (c) applies.[33] In turn, section 2703 specifically empowers the government to "require the *disclosure* by a provider . . . of the contents of a[n] . . .

---

[28] 18 U.S.C. § 2701

[29] *Id.* § 2701(c)(1) (emphasis added).

[30] The panel majority characterizes a service provider that "access[es]" a user's email pursuant to an SCA warrant as "an agent of the government." Majority Op. at 29, 39. But, the legal authorities cited by the panel for the proposition that a private party who assists the government in conducting a search and seizure "becomes an agent of the government," *id.* at 29, do not involve circumstances, such as those here, where the private party already had possession of the relevant property.

[31] *Id.* §§ 2702-03 (emphasis added).

[32] *See id.* § 2702(a)(1)-(3).

[33] *Id.* (emphasis added).

electronic communication . . . pursuant to a warrant."[34]

Considering sections 2701, 2702, and 2703 together, it is clear that the SCA protects user privacy by prohibiting unlawful access of customer communications (such as hacking), and by regulating a provider's *disclosure* of customer communications to third parties. Inasmuch as section 2701's limitations on *access* specifically do not apply to providers, it is only when a provider *divulges* the content of a user's communication to a third party that the provider puts a user's privacy at risk. It is not a mere coincidence that the SCA recognizes a provider's standing authority to *access* a user's communications and, at the same time, prohibits a provider from *disclosing* those communications to third-parties except as authorized by sections 2702 and 2703. Accordingly, the panel majority's focus on *access* (instead of on *disclosure)* is entirely misplaced.[35]

---

[34] *Id.* § 2703(a) (emphasis added).

[35] Neither the panel majority's opinion nor the *en banc* concurrence explains why "privacy" is better served by looking to a provider's *access* rather than its *disclosure*. They just assume the point. *See ante* at 13 (Carney, *J.*, concurring in the order denying reh'g *en banc*) ("The better approach . . . is one that looks to the step taken before disclosure—access—in determining privacy's territorial locus."); Majority Op. at 39. Both the panel majority's opinion and the *en banc* concurrence also fail to explain why the physical location of the datacenter is the legal point of *access*, rather than the location from where the service provider electronically gains *access* to the targeted data, which, in this case, is the United States. Evidently, it is so (again) because the panel majority and the concurrence say it is so. *See ante* at 4 (Carney, *J.*, concurring in the order denying reh'g *en banc*) ("[T]he locus of the SCA's privacy protections [is] at the place of data storage.");

Put another way, Microsoft did not need a warrant to take possession of the emails stored in Ireland. Nor did it need a warrant to move the emails from Ireland to the United States. It already had possession of, and lawful *access* to, the targeted emails from its office in Redmond, Washington. Only Microsoft's *disclosure* of the emails to the government would have been unlawful under the SCA absent a warrant.[36]

* * *

In sum, the government obtained a warrant based on a showing of probable cause before a judicial officer of the United States. That warrant required Microsoft's office in Redmond, Washington, to disclose certain emails that happened to be electronically stored in its servers abroad, but to which Microsoft had immediate access in the United States. Because the location of a provider's *disclosure* determines whether the SCA is applied domestically or extraterritorially, the enforcement of the warrant here involved a domestic application of the SCA. The panel should have affirmed the District Court's denial of Microsoft's motion to quash.

Majority Op. at 39. Naked assertions, however, do not the law make.

[36] To the extent the panel majority concludes that the SCA does not apply extraterritorially to compel a provider's disclosures pursuant to section 2703, its place-of-access reasoning raises concerns about the extraterritorial reach of protections from unlawful access and disclosures afforded by sections 2701 and 2702. Such a concern might be avoided if the statute is construed to reach, at least, the conduct of persons within the jurisdiction of the United States. This further concern only reinforces the need for *en banc* review.

For the foregoing reasons, I dissent from the order denying rehearing *en banc*. I trust that the panel's misreading of this important statute can be rectified as soon as possible by a higher judicial authority or by the Congress of the United States.[37]

---

[37] Ultimately, Judge Carney's concurring opinion suggests that rehearing *en banc* is unnecessary because the panel majority's holding was compelled by an anachronistic statute and an inflexible framework for analyzing questions of extraterritoriality. *Ante* at 13-14 (Carney, *J.*, concurring in the order denying reh'g *en banc*). It also notes that some Members of Congress have introduced a bill purporting to resolve all of our concerns with the statute. *Id.* at 2 n.3. I submit that rehearing *en banc* is necessary precisely because the panel majority misread the SCA and misapplied the extraterritoriality framework set forth in *Morrison*. Where a decision of our court has unnecessarily created serious, on-going problems for those charged with enforcing the law and ensuring our national security, and where a legislative remedy is entirely speculative, we should not shirk our duty to interpret an extant statute in accordance with its terms.

REENA RAGGI, *Circuit Judge*, joined by DENNIS JACOBS, JOSÉ A. CABRANES, and CHRISTOPHER F. DRONEY, *Circuit Judges*, dissenting from the order denying rehearing *en banc*:

In this case, a panel of the court quashes a compelled-disclosure warrant issued under the Stored Communications Act ("SCA") by a neutral magistrate and supported by probable cause to think that the information demanded is evidence of a crime. *See* 18 U.S.C. § 2703(a). The ground for decision is the presumption against extraterritoriality, *see Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. 247, 255 (2010), which the panel construes to allow United States corporation Microsoft to refuse to disclose subscriber communications in its possession and responsive to the warrant because Microsoft, for its own business reasons and unbeknownst to its subscriber, has chosen to store the communications in Ireland. The panel does not simply set a *higher* bar for the government to secure such electronic communications. Rather, it erects an "*absolute*" bar so that "the government can never obtain a warrant that would require Microsoft," or any other U.S.-based service provider, to turn over electronic communications stored abroad, "however certain it may be that they contain evidence of criminal activity, and even if that criminal activity is a terrorist plot." *Microsoft Corp. v. United States* ("*Microsoft*"), 829 F.3d 197, 224 (2d Cir. 2016) (Lynch, J., concurring in the judgment) (emphasis in original).[1] This ruling merits

---

[1] On the panel's reasoning, if on September 10, 2001, the government had been able to show probable cause to believe that Mohamed Atta, Abdul Aziz al Omari, etc., were communicating electronically about an imminent, devastating attack on the United States, and

en banc review. To the extent an equally divided court today denies such review, I respectfully dissent.

1. Matter of Exceptional Importance

The panel's ruling, the reasoning informing it, and its disturbing consequences raise questions "of exceptional importance to public safety and national security." Cabranes, J., Op. Dissenting from Denial of Reh'g En Banc ("Cabranes, J., Op."), *ante* at 1. The panel nevertheless urges us to forego *en banc* review because the SCA is outdated and overdue for congressional revision. *See Microsoft*, 829 F.3d at 201; Carney, J., Op. Concurring in Denial of Reh'g En Banc ("Carney, J., Op."), *ante* at 2 & n.3. I am not persuaded.

This is not a case where some legal principle (*e.g.*, standing, mootness) allowed the panel to avoid applying the SCA, thereby affording Congress time to enact new legislation. This is a case where the panel reached the merits and construed the SCA to foreclose altogether § 2703(a) warrants requiring United States service providers to disclose electronic communications stored overseas. This construction now controls the SCA's application in this circuit. In its Petition for Rehearing, the government details the immediate and serious adverse consequences of such a ruling. *See* Gov't Pet. for Reh'g at 18-19; *see also* Cabranes, J., Op., *ante* at 2-7. These consequences cannot be attributed to deficiencies in the SCA. Rather, they derive from the panel's conclusion—mistaken in my view—that the

---

that Microsoft possessed those emails, no federal court could have issued a § 2703(a) warrant compelling Microsoft to disclose those emails if it had stored them overseas, even though its employees would not have had to leave their desks in Redmond, Washington, to retrieve them.

SCA is impermissibly being applied extraterritorially when a § 2703(a) warrant requires a United States service provider to disclose electronic communications that it has elected to store abroad. It is simply unprecedented to conclude that the presumption against extraterritoriality bars United States courts with personal jurisdiction over a United States person from ordering that person to produce property in his possession (wherever located) when the government has made a probable cause showing that the property is evidence of a crime. This alone warrants *en banc* review.

2. The Panel's Discussion of "Warrant"

Several aspects of the panel's extraterritoriality analysis require particular review. The first is the panel's lengthy discussion of why Congress's "use of the term of art 'warrant'" in the SCA manifests an intent for the statute to operate only domestically. *Microsoft*, 829 F.3d at 212. At the outset, I note that there was no need for the panel to locate *domestic* intent in the SCA; it is presumed in the absence of a showing of express *extraterritorial* intent, which the government concedes is absent here. *See Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. at 255. The panel majority's "warrant" discussion, however, is not simply unnecessary. It is also flawed in ways that lay an unsound foundation for the panel's ensuing identification of statutory "focus."

Notably, the panel majority concludes that Congress's use of the term "warrant" in § 2703 signals its intent to invoke all of the "traditional, domestic Connotations" that pertain to traditional search warrants. *Microsoft*, 829 F.3d at 213. But, as Judge Lynch observes, a § 2703(a) warrant is not a traditional war-

rant. *Id.* at 226 (Lynch, J., concurring in the judgment). It does not authorize federal agents to *search* any premises or to *seize* any person or materials. Rather, it authorizes a federal agent to require a service provider to disclose materials in its possession. The difference is significant to identifying where a warrant is being executed. Because a search warrant is executed with respect to a *place*—the place to be searched—the presumption against extraterritoriality expects that place to be within United States territory. By contrast, because a § 2703(a) warrant is executed with respect to a *person*—the person ordered to divulge materials in his possession—the presumption against extraterritoriality expects that person to be within United States territory and subject to the court's jurisdiction. If the person is so present, execution of the warrant as to him is a domestic application of United States law without regard to from where the person must retrieve the materials ordered disclosed. Indeed, if that were not so, subpoenas requiring persons in this country to produce materials that they must retrieve from abroad could not be enforced, a position contrary to well established law. *See, e.g.*, *Marc Rich & Co., A.G. v. United States*, 707 F.2d 663, 668-70 (2d Cir. 1983); *United States v. Bank of Nova Scotia (In re Grand Jury Proceedings)*, 740 F.2d 817, 826-29 (11th Cir. 1984).

Thus, I respectfully submit that the panel majority's extraterritoriality analysis starts with the mistaken equation of § 2703(a) warrants with traditional search warrants. This, in turn, leads to the mistaken conclusion that "a warrant protects privacy in a distinctly territorial way." *Microsoft*, 829 F.3d at 212.

As to the latter point, the reason United States search warrants do not apply extraterritorially has to do with *sovereignty*, not *privacy*. Since before the republic, the law of nations has recognized that one sovereign cannot unilaterally enforce its criminal laws within the territory of another.[2] But a defendant's expectations of privacy do not preclude evidence so obtained from being used in a United States prosecution. *See In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157, 176-77 (2d Cir. 2008). Thus, it is respect for sovereign independence that has prompted us to observe that "search warrants intended to have extraterritorial effect . . . would have dubious legal significance, if any, in a foreign nation." *Id.* at 171. But this observation, quoted by the panel majority, does not support its ensuing conclusion that, "[a]ccordingly, a warrant protects *privacy* in a distinctly territorial way." *Microsoft*, 829 F.3d at 212 (emphasis added).

---

[2] *See* Restatement (Third) of Foreign Relations Law § 432(2) ("A state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state, given by duly authorized officials of that state."); 1 *Oppenheim's International Law* § 119 (Robert Jennings & Arthur Watts, eds., 9th ed. 1992) ("It is . . . a breach of international law for a state without permission to send its agents into the territory of another state to apprehend persons accused of having committed a crime."); *The Apollon*, 22 U.S. (9 Wheat.) 362, 371 (1824) (Story, J.) (holding that "[i]t would be monstrous to suppose that our revenue officers were authorized to enter into foreign ports and territories, for the purpose of seizing vessels which had offended against our laws" because such conduct would be "a clear violation of the laws of nations"); *The Nereide*, 13 U.S. (9 Cranch) 388, 423 (1815) (Marshall, C.J.) ("[T]he Court is bound by the law of nations which is a part of the law of the land.").

As Judge Lynch explains, how warrants protect *privacy* is through the Fourth Amendment requirement that they issue only "upon probable cause." U.S. Const. amend. IV; *see Microsoft*, 829 F.3d at 223 (Lynch, J., concurring in the judgment). Indeed, to the extent the SCA's legislative history shows Congress's intent to extend privacy protections, specifically, protections "analogous to those provided by the Fourth Amendment," to certain electronic communications, *Microsoft*, 829 F.3d at 206 (quoting Gov't Br. at 29), one might better understand Congress to have used the term "warrant" in § 2703(a) to ensure that certain disclosures would be compelled only upon a showing of probable cause. Thus, when a § 2703(a) warrant supported by probable cause is executed on a person within the jurisdiction of the United States, the SCA is being applied domestically without regard to the location of the materials that the person must divulge.

As Judge Cabranes observes, by failing to recognize these distinctions (a) between search warrants directed to particular locations and § 2703(a) warrants directed to particular persons, and (b) between the values of sovereignty and privacy, the panel majority construes "warrant" as used in § 2703 to yield a perverse result: affording *greater* privacy protection to foreign citizens and Americans who claim to reside abroad than to resident U.S. citizens. *See* Cabranes, J., Op., *ante* at 7-8 n.19. This troubling result and the reasons leading to it warrant *en banc* review.

3. The Focus of the Statute

Where, as here, the government does not argue that Congress intended for § 2703(a) to apply extraterritorially, the determinative question asks whether the

domestic contacts associated with that statutory provision are sufficient to avoid triggering the presumption against extraterritoriality. To answer that question, a court looks to "the territorial events or relationships" that are the "focus" of the relevant statutory provision. *Mastafa v. Chevron Corp.*, 770 F.3d 170, 184 (2d Cir. 2014) (alterations omitted); *Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. at 266-68. The panel majority identifies "privacy" as the focus of § 2703(a)'s warrant requirement. *Microsoft*, 829 F.3d at 217. It then reasons that because the § 2703(a) warrant here sought disclosure of the electronic communications of a Microsoft customer, and because Microsoft stored those communications in Dublin, "[t]he content to be *seized* is stored in Dublin." *Id.* at 220 (emphasis added). This in turn leads it to conclude that "the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed—here, where it is *seized by Microsoft, acting as an agent of the government.*" *Id.* (emphasis added). Accordingly, it concludes that the § 2703(a) warrant is being executed in Ireland in violation of the presumption against extraterritoriality.

This reasoning raises several concerns.

First, I cannot agree that a person who is compelled by a § 2703(a) warrant to disclose to the government materials already in that person's possession is "seiz[ing]" anything as an agent of the government. *See id.* The cases cited by the panel majority identify such agency where property is *not* already in an actor's possession. In such circumstances, but for authorizing law or warrant, the actor could not lawfully take possession of—*i.e.*, seize—third-party materials. That is not the

case here. Microsoft did not need any warrant from the United States to take possession of the subscriber communications it had stored in Ireland. Nor did it need such a warrant to transfer those communications from Ireland to the United States. Indeed, it did not need the approval of Irish authorities or even of its subscriber to take such action. Thus, it is simply wrong to characterize Microsoft's actions in retrieving customer electronic data in Ireland as "Microsoft's *execution* of the warrant," much less as a *seizure* by Microsoft. Carney, J., Op., *ante* at 3 (emphasis added); *see Microsoft*, 829 F.3d at 220. The § 2703(a) warrant here at issue was executed by *federal authorities*, who were thereby authorized to compel Microsoft to *disclose* communications already lawfully in its possession. Such disclosure by Microsoft would otherwise have been prohibited by 18 U.S.C. § 2702(a). But the only territorial event that needs to be warranted under the SCA is disclosure. No warrant was needed for Microsoft lawfully to access material on its Dublin servers from the United States. Nor is a different conclusion supported by the panel majority's observation that our court "has never upheld the use of a subpoena to compel a recipient to produce an item under its control and located overseas when the recipient is merely a caretaker for another individual or entity and that individual, not the subpoena recipient, has a protectable privacy interest in the item." *Microsoft*, 829 F.3d at 215. The question whether the caretaker's actions respecting materials in his possession constitute a "search" or "seizure" undertaken as an agent of the government does not turn on whether the item is located here or overseas. Indeed, as Judge Lynch states, we have upheld the use of a subpoena to compel a caretaker to

produce client materials in its domestic possession. *See id.* at 228 n.5 (Lynch, J., concurring in the judgment) (citing *In re Horowitz*, 482 F.2d 72 (2d Cir. 1973)). Such a conclusion would not have been possible if the caretaker's actions respecting materials in his possession equated to a "search" or "seizure" undertaken as an agent of the government.

Thus, we need to convene *en banc* to clarify that a service provider who complies with a § 2703(a) warrant compelling disclosure of communications in his lawful possession does not thereby conduct a search or seizure as the agent of the government.

Second, I also cannot agree with the panel that *privacy* is the focus of § 2703 and that subscriber privacy would be invaded *in Ireland* were Microsoft to access its subscriber files there. To the extent § 2702(a) generally prohibits a service provider from knowingly disclosing subscribers' electronic communications to third parties, that provision might be understood to focus on enhancing subscriber privacy. But § 2703 identifies circumstances when the government nevertheless "may require" service providers to disclose their subscribers' communications. This gives some force to the government's argument that the focus of § 2703 is compelled *disclosure*, not enhanced *privacy*. *See* Gov't Pet. for Reh'g at 11-12 (noting that focus inquiry is "provision-specific" and citing *RJR Nabisco, Inc. v. European Cmty.*, 136 S. Ct. 2090, 2101-11 (2016)). *But see Microsoft*, 829 F.3d at 218-19 (rejecting disclosure focus argument).

Even assuming that the enhanced privacy and compelled disclosure provisions of the SCA are two sides of the same coin, I think the panel errs in concluding that

the privacy afforded by the SCA would be invaded by Microsoft's access of its own files in Dublin rather than by its subsequent disclosure of subscriber communications in the United States.

As already stated, Microsoft is entitled to access and to move subscriber communications at will, even without consulting its subscriber. Such actions by Microsoft disclose nothing to the government about the existence or content of such communications. The only privacy interest afforded by § 2702(a), however, is against such disclosure. The statute provides no privacy right against Microsoft's own handling of communications short of such disclosure. Thus, contrary to the panel, I think that, even if privacy is the focus of §§ 2702 and 2703, the territorial event that is the focus of that privacy interest is the service provider's disclosure of the subscriber communications to a third party —whether in violation of § 2702(a) or as authorized by warrant under § 2703(a). It is where that disclosure occurs that determines whether these statutory provisions are being applied domestically or extraterritorially.

Here, there is no question that the challenged § 2703(a) warrant issued, was served on Microsoft in, and required disclosure in the United States. Thus, even if "privacy" is the statute's "focus," the challenged warrant here applies the statute domestically, not extraterritorially. We should say so *en banc*.

4. Concluding Observations

Two final points. As Judge Cabranes observes, and Judge Carney seems to agree, the same reasoning that leads the panel to conclude that § 2703(a) warrants

cannot reach communications that Microsoft has stored in Ireland might also preclude affording § 2702(a) privacy protections to such materials. *See* Cabranes, J., Op., *ante* at 14 n.36; Carney, J., Op., *ante* at 7 n.6. But if § 2702(a) protections do not apply here, does the government even need a § 2703(a) warrant? Could it simply proceed by subpoena? *See Marc Rich & Co., A.G. v. United States*, 707 F.2d at 668-70; *United States v. Bank of Nova Scotia (In re Grand Jury Proceedings)*, 740 F.2d at 826-29. I think the government does need a § 2703(a) warrant because I understand both § 2702(a) protections and § 2703(a) warrants to exercise government authority domestically on persons subject to United States jurisdiction. To the extent, however, that the panel's extraterritoriality reasoning might allow a United States service provider such as Microsoft to flout not only § 2703(a) warrants but also § 2702(a) protections simply by moving materials abroad, the need for *en banc* review is only heightened.

My second point is not unrelated. The panel concludes that, because the Congress that enacted the SCA could not have foreseen the technological context in which this case arises, the focus of the statute cannot be domestic disclosure of data that a service provider in the United States accesses from abroad. Therefore, the warrant should be quashed. It seems to me this allows the first prong of analysis—did Congress intend extraterritoriality?—to be determinative of the second—is the statute being applied extraterritorially in the case at hand? In fact, the two steps of analysis are distinct. *See Morrison v. Nat'l Australia Bank Ltd.*, 561 U.S. at 266. Whatever Congress may have foreseen about advances in electronic communications, I think, for the reasons already stated, that the SCA is

being applied domestically here. The privacy protection afforded by § 2702(a) is against unauthorized *disclosure* to third parties. But a § 2703(a) warrant here specifically authorizes federal agents to compel disclosure in the United States. Further, the party from whom such disclosure is being compelled is a United States service provider subject to the personal jurisdiction of United States courts. In short, this is not the case hypothesized by the panel where the government might use a § 2703(a) warrant to demand communications *stored abroad* from a *foreign service provider* relating to a *foreign subscriber*. *See, e.g.*, *Microsoft*, 829 F.3d at 231-32 (Lynch, J., concurring in the judgment); Carney, J., Op., *ante* at 8-9. When such a case comes before us, we can certainly consider whether a court with personal jurisdiction over the foreign service provider can issue a § 2703(a) warrant compelling it to disclose in the United States communications stored abroad. But, in this case, where the warrant is directed to a United States provider over whom there is personal jurisdiction for production in the United States of specified communications on a federal magistrate's identification of probable cause, I simply do not think we have an extraterritorial application of U.S. law.

For the foregoing reasons, this court *en banc* should enforce, not quash, the challenged § 2703(a) warrant.

CHRISTOPHER F. DRONEY, *Circuit Judge*, joined by DENNIS JACOBS, JOSÉ A. CABRANES, and REENA RAGGI, *Circuit Judges*, dissenting from the denial of rehearing *en banc*:

The majority opinion undertook the daunting task of attempting to apply a statute enacted decades ago to present technology. For example, who knew in 1986 that electronic mail—"email"—would become such a primary means of communication that its commercial providers would have millions of servers across the world to store and manage those communications? Or that the recipient of the warrant here—Microsoft—would itself manage over one million server computers, located in over forty countries, used by over one billion customers? Such developments in electronic communications could not have been anticipated at the time of the statute's adoption. Indeed, the task of applying statutes and rules from many years ago to unanticipated advances in technology has been undertaken in other contexts with much difficulty. *See, e.g.*, *United States v. Ganias*, 824 F.3d 199, 219-21 (2d Cir. 2016) (*en banc*). Thus, although I agree that reconsideration *en banc* should have occurred, I do so while recognizing the majority's efforts to solve the vexing issues presented here.

I dissent, though, from the denial of *en banc* in this case for three reasons. First, the privacy interests that are the focus of many aspects of the Stored Communications Act ("SCA") are protected in this context by its warrant requirement. Second, the activity that is the focus of the disclosure aspects of the SCA would necessarily occur in the United States where Microsoft is headquartered and where it would comply with the

§ 2703 warrant, not in the foreign country where it has chosen to store the electronic communications of its customers; also, the provisions of the statute concerning the mechanics of disclosure of these communications are unrelated to its privacy provisions. Third, the prudent course of action is to allow the warrants to proceed, and if Congress wishes to change the statute, it may do so while important criminal investigations continue.

When determining whether a statute applies extraterritorially, a court must read the statute provision by provision, not as a whole. *RJR Nabisco, Inc. v. European Community*, 136 S. Ct. 2090, 2103 (2016) (analyzing provisions individually to determine the focus of each). The court is then tasked with "determin[ing] whether the case involves a domestic application of the statute, and [does] this by looking to the statute's 'focus.'" *Id.* at 2101.

As the majority opinion notes, the SCA was broadly focused on the privacy concerns of electronic communications and the parties to those communications. *See* Maj. Op. at 33-36. But Congress addressed those concerns through the warrant requirement in the SCA. *See* 18 U.S.C. § 2703. That requirement provides protection for individual privacy interests by requiring the Government to make an adequate showing of probable cause of evidence of a crime or property used to commit a crime to a judge—a well-established standard of Fourth Amendment protection. *See id.*; Fed. R. Crim. P. 41(c); U.S. Const. amend. IV ("[N]o warrants shall issue, but upon probable cause."); *Camara v. Mun. Court of City & Cnty. of S.F.*, 387 U.S. 523, 528 (1967) (explaining that purpose of Fourth Amendment's

probable cause requirement "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials").

Furthermore, the provisions of the SCA concerning the means of disclosure following obtaining the warrant are quite separate from the privacy components of the SCA. Section 2703 includes a number of specific disclosure provisions, which state it is the *provider* of the electronic communication service that is the source of the records sought by the Government either pursuant to the warrant or the other means provided by that section to properly obtain the electronic communications. *See id.* § 2703 (a) ("A governmental entity may require the disclosure *by a provider* of electronic communication service of the contents of a wire or electronic communication . . . .") (emphasis added); § 2703 (b)(1) ("A governmental entity may require *a provider* of remote computing service to disclose the contents of any wire or electronic communication . . .") (emphasis added); § 2703 (c)(1) & (2) (both describing disclosure by providers); § 2703 (g) (same).

Thus, the only permissible reading of § 2703 is that it is the location of the provider of the electronic communication service that is relevant to determining whether the SCA is being applied extraterritorially under *RJR Nabisco*. Microsoft is headquartered in the United States, and there is no question that it would make the disclosure mandated by the § 2703 warrant in this country.

It makes no difference that Microsoft has chosen to store some electronic communications in other countries. That decision is based on its own business considerations, not privacy concerns for its customers.

Microsoft has possession and immediate access to those emails regardless of where it chose to store them. Thus, the second prong of the *RJR Nabisco* test is satisfied here: the disclosure of the electronic communications occurs in the United States, when Microsoft honors the warrant by disclosing those communications.

It is also important to note that the interests of foreign internet electronic communication service providers, whose headquarters are abroad and whose customers choose to subscribe to those services with the knowledge that the provider is located outside the United States, are not at stake here. If the emails sought by the Government in this case were maintained by a foreign-based internet service provider, the situation would be quite different. Here, however, the majority's concerns regarding "the interests of comity that . . . ordinarily govern the conduct of cross- boundary criminal investigations," Maj. Op. at 42, are overstated when the warrant is served on a U.S.-based electronic communication service provider for stored emails of a customer who *chose* to have a U.S.-based electronic communication service provider furnish his email service.

There is a real and practical component to the denial of *en banc* review of this case. This is a case that turns on statutory interpretation under *RJR Nabisco* rather than responding to a direct challenge to the constitutionality of the SCA or its disclosure provisions. The denial of *en banc* review hobbles both this specific Government investigation as well as many others, important not only to the United States but also foreign nations. The Government's interest in contin-

uing critical investigations into criminal activity is manifest. If Congress wishes to revisit the privacy and disclosure aspects of § 2703, it is free to do so when it chooses to do so. Until that time, this Court should allow the warrants to compel disclosure pursuant to § 2703 as it exists, and allow the Government to do its job in investigating serious criminal activity.

For these reasons, I respectfully dissent from the denial of *en banc* review.

APPENDIX G

1. 18 U.S.C. 2701 provides:

Unlawful access to stored communications

(a) OFFENSE.—Except as provided in subsection (c) of this section whoever—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) intentionally exceeds an authorization to access that facility;

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) PUNISHMENT.—The punishment for an offense under subsection (a) of this section is—

(1) if the offense is committed for purposes of commercial advantage, malicious destruction or damage, or private commercial gain, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State—

(A) a fine under this title or imprisonment for not more than 5 years, or both, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and

(2) in any other case—

(A) a fine under this title or imprisonment for not more than 1 year or both, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) EXCEPTIONS.—Subsection (a) of this section does not apply with respect to conduct authorized—

(1) by the person or entity providing a wire or electronic communications service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 2703, 2704 or 2518 of this title.

2. 18 U.S.C. 2702 (2012) provides:

Voluntary disclosures of customer communications or records

(a) PROHIBITIONS.—Except as provided in subsection (b) or (c)—

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any com-

munication which is carried or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS.—A provider described in subsection (a) may divulge the contents of a communication—

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such commu-

nication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency—

(A) if the contents—

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

[(B) Repealed. Pub. L. 108-21, title V, § 508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.

(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS.—A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))—

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A; or

(6) to any person other than a governmental entity.

(d) REPORTING OF EMERGENCY DISCLOSURES.—On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing—

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8); and

(2) a summary of the basis for disclosure in those instances where—

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges.

3. 18 U.S.C. 2703 provides:

Required disclosure of customer communications or records

(a) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN ELECTRONIC STORAGE.—A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) CONTENTS OF WIRE OR ELECTRONIC COMMUNICATIONS IN A REMOTE COMPUTING SERVICE.—(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection—

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity—

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service—

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) RECORDS CONCERNING ELECTRONIC COMMUNICATION SERVICE OR REMOTE COMPUTING SERVICE. —(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may

quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) NO CAUSE OF ACTION AGAINST A PROVIDER DISCLOSING INFORMATION UNDER THIS CHAPTER.—No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) REQUIREMENT TO PRESERVE EVIDENCE.—

(1) IN GENERAL.—A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) PERIOD OF RETENTION.—Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) PRESENCE OF OFFICER NOT REQUIRED.—Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other

information pertaining to a subscriber to or customer of such service.

4. 18 U.S.C. 2711 provides:

Definitions for chapter

As used in this chapter—

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section;

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system;

(3) the term "court of competent jurisdiction" includes—

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that—

(i) has jurisdiction over the offense being investigated;

(ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or

(iii) is acting on a request for foreign assistance pursuant to section 3512 of this title; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants; and

(4) the term "governmental entity" means a department or agency of the United States or any State or political subdivision thereof.